

From: [Griffin, Mark](#)
To: [Racine, Karl](#); [Wilhelm, Abby Jae](#); [Fitzgerald, Patricia M. \(USAOHN\)](#); [Mygatt, Timothy \(CRT\)](#)
Cc: [Thomas, Delante](#); [Anderson, Leigh Ph.D](#); [Drummond, Dornat](#); [Todd, Dorothy](#); [Carney, Brian](#); [Johnson, Carlos](#); [Yonekura, Stephanie](#); [Caruso, Courtney](#); [Christine Cole](#); [Ronnie Dunn](#); [Coromelas, Acrivi \(CRT\)](#); [Geissler, Jonas \(CRT\)](#); [Heyer, Michelle L. \(USAOHN\)](#); [DeCaro, Sara \(USAOHN\)](#); [Evanovich, Michael \(USAOHN\) \[Contractor\]](#); [Wilhelm, Abby Jae](#); [Puin, Timothy](#)
Subject: [EXTERNAL] RE: Access to Unredacted Documents -- Need for Clarifying Order
Date: Wednesday, January 10, 2024 9:31:00 AM
Attachments: [Emails with BCI and DPS re MT.pdf](#)

Karl – here’s what we have so far. Not sure that there is anything more, but we will supplement if so.

From: Griffin, Mark
Sent: Wednesday, January 10, 2024 9:20 AM
To: [Racine, Karl](#) <karl.racine@hoganlovells.com>; [Wilhelm, Abby Jae](#) <abby.wilhelm@hoganlovells.com>; [Fitzgerald, Patricia M. \(USAOHN\)](#) <Patricia.Fitzgerald2@usdoj.gov>; [Mygatt, Timothy \(CRT\)](#) <Timothy.Mygatt@usdoj.gov>
Cc: [Thomas, Delante](#) <dtomas3@clevelandohio.gov>; [Anderson, Leigh Ph.D](#) <LAnderson2@clevelandohio.gov>; [Drummond, Dornat](#) <ddrummond@clevelandohio.gov>; [Todd, Dorothy](#) <DTodd@clevelandohio.gov>; [Carney, Brian](#) <BCarney@clevelandohio.gov>; [Johnson, Carlos](#) <CJohnson2@clevelandohio.gov>; [Yonekura, Stephanie](#) <stephanie.yonekura@hoganlovells.com>; [Caruso, Courtney](#) <courtney.caruso@hoganlovells.com>; [Christine Cole](#) <christinecole919@gmail.com>; [Ronnie Dunn](#) <rdunn6682@gmail.com>; [Coromelas, Acrivi \(CRT\)](#) <Acrivi.Coromelas2@usdoj.gov>; [Geissler, Jonas \(CRT\)](#) <Jonas.Geissler@usdoj.gov>; [Heyer, Michelle L. \(USAOHN\)](#) <Michelle.Heyer@usdoj.gov>; [DeCaro, Sara \(USAOHN\)](#) <Sara.DeCaro@usdoj.gov>; [Evanovich, Michael \(USAOHN\) \[Contractor\]](#) <Michael.Evanovich@usdoj.gov>; [Wilhelm, Abby Jae](#) <abby.wilhelm@hoganlovells.com>
Subject: RE: Access to Unredacted Documents -- Need for Clarifying Order

Thanks, Karl. I have asked the team to look for the requested documents.

From: [Racine, Karl](#) <karl.racine@hoganlovells.com>
Sent: Tuesday, January 9, 2024 7:18 PM
To: [Wilhelm, Abby Jae](#) <abby.wilhelm@hoganlovells.com>; [Fitzgerald, Patricia M. \(USAOHN\)](#) <Patricia.Fitzgerald2@usdoj.gov>; [Griffin, Mark](#) <MGriffin@clevelandohio.gov>; [Mygatt, Timothy \(CRT\)](#) <Timothy.Mygatt@usdoj.gov>
Cc: [Thomas, Delante](#) <dtomas3@clevelandohio.gov>; [Anderson, Leigh Ph.D](#) <LAnderson2@clevelandohio.gov>; [Drummond, Dornat](#) <ddrummond@clevelandohio.gov>; [Todd, Dorothy](#) <DTodd@clevelandohio.gov>; [Carney, Brian](#) <BCarney@clevelandohio.gov>; [Johnson, Carlos](#) <CJohnson2@clevelandohio.gov>; [Yonekura, Stephanie](#) <stephanie.yonekura@hoganlovells.com>; [Caruso, Courtney](#) <courtney.caruso@hoganlovells.com>; [Christine Cole](#) <christinecole919@gmail.com>; [Ronnie Dunn](#) <rdunn6682@gmail.com>; [Coromelas, Acrivi \(CRT\)](#) <Acrivi.Coromelas2@usdoj.gov>; [Geissler, Jonas \(CRT\)](#) <Jonas.Geissler@usdoj.gov>; [Heyer, Michelle L. \(USAOHN\)](#) <Michelle.Heyer@usdoj.gov>; [DeCaro, Sara \(USAOHN\)](#) <Sara.DeCaro@usdoj.gov>; [Evanovich, Michael \(USAOHN\) \[Contractor\]](#) <Michael.Evanovich@usdoj.gov>; [Wilhelm, Abby Jae](#) <abby.wilhelm@hoganlovells.com>

GOVERNMENT
EXHIBIT

2

Subject: RE: Access to Unredacted Documents -- Need for Clarifying Order

Mark:

I am writing to reiterate DOJ and Abby's request for any and all written correspondence the City has had with the relevant authorities (LEADS administrators, the Ohio AG's office, and anyone else) in regards to accessing unredacted documents. Please provide these materials by end of business Thursday, January 11.

As you know, the inability to access IAPro and Evidence.com effectively precludes the Monitoring Team from performing its work.

Best,
Karl

Karl A. Racine

Partner

Hogan Lovells US LLP

Columbia Square

555 Thirteenth Street, NW

Washington, DC 20004-1109

Tel: [+1 202 637 5600](tel:+12026375600)

Direct: [+1 202 637 5861](tel:+12026375861)

Fax: [+1 202 637 5910](tel:+12026375910)

Email: karl.racine@hoganlovells.com

www.hoganlovells.com

From: Wilhelm, Abby Jae <abby.wilhelm@hoganlovells.com>

Sent: Monday, January 8, 2024 8:38 AM

To: Fitzgerald, Patricia M. (USAOHN) <Patricia.Fitzgerald2@usdoj.gov>; Griffin, Mark <MGriffin@clevelandohio.gov>; Racine, Karl <karl.racine@hoganlovells.com>; Mygatt, Timothy (CRT) <Timothy.Mygatt@usdoj.gov>

Cc: Thomas, Delante <dthomas3@clevelandohio.gov>; Anderson, Leigh Ph.D <LAnderson2@clevelandohio.gov>; Drummond, Dornat <ddrummond@clevelandohio.gov>; Todd, Dorothy <DTodd@clevelandohio.gov>; Carney, Brian <BCarney@clevelandohio.gov>; Johnson, Carlos <CJohnson2@clevelandohio.gov>; Yonekura, Stephanie <stephanie.yonekura@hoganlovells.com>; Caruso, Courtney <courtney.caruso@hoganlovells.com>; Christine Cole <christinecole919@gmail.com>; Ronnie Dunn <rdunn6682@gmail.com>; Coromelas, Acrivi (CRT) <Acrivi.Coromelas2@usdoj.gov>; Geissler, Jonas (CRT) <Jonas.Geissler@usdoj.gov>; Heyer, Michelle L. (USAOHN) <Michelle.Heyer@usdoj.gov>; DeCaro, Sara (USAOHN) <Sara.DeCaro@usdoj.gov>; Evanovich, Michael (USAOHN) [Contractor] <Michael.Evanovich@usdoj.gov>

Subject: RE: Access to Unredacted Documents -- Need for Clarifying Order

Good Morning, Mark:

I am following up on the below request from DOJ. Can you please provide the relevant/written

correspondence for us to review? I'd like to get this meeting scheduled as soon as possible.

Thank you in advance,
Abby

From: Fitzgerald, Patricia M. (USAOHN) <Patricia.Fitzgerald2@usdoj.gov>
Sent: Wednesday, January 3, 2024 1:55 PM
To: Griffin, Mark <MGriffin@clevelandohio.gov>; Racine, Karl <karl.racine@hoganlovells.com>; Mygatt, Timothy (CRT) <Timothy.Mygatt@usdoj.gov>
Cc: Wilhelm, Abby Jae <abby.wilhelm@hoganlovells.com>; Thomas, Delante <dthomas3@clevelandohio.gov>; Anderson, Leigh Ph.D <LAnderson2@clevelandohio.gov>; Drummond, Dornat <ddrummond@clevelandohio.gov>; Todd, Dorothy <DTodd@clevelandohio.gov>; Carney, Brian <BCarney@clevelandohio.gov>; Johnson, Carlos <CJohnson2@clevelandohio.gov>; Yonekura, Stephanie <stephanie.yonekura@hoganlovells.com>; Caruso, Courtney <courtney.caruso@hoganlovells.com>; Christine Cole <christinecole919@gmail.com>; Ronnie Dunn <rdunn6682@gmail.com>; Coromelas, Acrivi (CRT) <Acrivi.Coromelas2@usdoj.gov>; Geissler, Jonas (CRT) <Jonas.Geissler@usdoj.gov>; Heyer, Michelle L. (USAOHN) <Michelle.Heyer@usdoj.gov>; DeCaro, Sara (USAOHN) <Sara.DeCaro@usdoj.gov>; Evanovich, Michael (USAOHN) [Contractor] <Michael.Evanovich@usdoj.gov>
Subject: RE: Access to Unredacted Documents -- Need for Clarifying Order

[EXTERNAL]

Hi Mark,

Happy New Year, and thanks for your email. We agree that that a meeting between the parties and the MT about these issues would be useful. To maximize the productivity of that discussion, DOJ requests that you share with us and the MT all written communications the City has had with state authorities (LEADS administrators, the Ohio AG's office, and anyone else) on this matter in advance of the meeting. This will help everyone understand the basis and the scope of the concerns around access to the information, and what has been tried so far to address them. Once we've had a change to digest that background, we would ask that Abby schedule a meeting.

Thanks,

Tricia Fitzgerald
(216) 622-3779

From: Griffin, Mark <MGriffin@clevelandohio.gov>
Sent: Friday, December 29, 2023 2:40 PM
To: Racine, Karl <karl.racine@hoganlovells.com>; Mygatt, Timothy (CRT) <Timothy.Mygatt@usdoj.gov>
Cc: Wilhelm, Abby Jae <abby.wilhelm@hoganlovells.com>; Fitzgerald, Patricia M. (USAOHN) <PFitzgerald@usa.doj.gov>; Thomas, Delante <dthomas3@clevelandohio.gov>; Anderson, Leigh Ph.D <LAnderson2@clevelandohio.gov>; Drummond, Dornat <ddrummond@clevelandohio.gov>; Todd, Dorothy <DTodd@clevelandohio.gov>; Carney, Brian <BCarney@clevelandohio.gov>; Johnson,

Carlos <CJohnson2@clevelandohio.gov>

Subject: [EXTERNAL] Access to Unredacted Documents -- Need for Clarifying Order

Karl and Tim,

The City would like to jointly approach Judge Oliver to request an order or other guidance clarifying that the Monitoring Team and the Department of Justice shall have unredacted access to all City criminal records, including criminal records otherwise protected by federal or state law (e.g. CJIS/LEADS protected information).

The City believes that the MT/DOJ should have access to unredacted law enforcement documents relevant to the Consent Decree. Much of this information is relevant to the City's compliance and progress under the Consent Decree.

However, federal and state law limit access to many of these documents for only specifically-permitted purposes. Accessing protected documents without a criminal justice purpose can have serious consequences. See, e.g. R.C. 2913.04.

Because of the ambiguity of these statutes, the City is pausing direct computer access to unredacted files in IA Pro and Evidence.com (and related files). As we have done with other files, the City will continue to provide redacted files as quickly as possible. It is my understanding that this has been an adequate – but not optimal – solution. But it is time-intensive and inserts unnecessary delays.

The City would prefer to not be required to redact documents. It is more efficient and more collaborative for the MT and DOJ to be provided direct access with the approval of Judge Oliver or other appropriate authority.

We would like to find a time to discuss these issues at your earliest convenience.

Best Regards,

Mark

About Hogan Lovells

Hogan Lovells is an international legal practice that includes Hogan Lovells US LLP and Hogan Lovells International LLP. For more information, see www.hoganlovells.com.

CONFIDENTIALITY. This email and any attachments are confidential, except where the email states it can be disclosed; it may also be privileged. If received in error, please do not disclose the contents to anyone, but notify the sender by return email and delete this email (and any attachments) from your system.

PRIVACY. Hogan Lovells processes personal data, including data relating to email communications, in accordance with the terms of its privacy policy which is available at www.hoganlovells.com/en/privacy.

From: [Puin, Timothy](#)
To: ["Zahid Siddiqi"](#)
Subject: Consent decree case redactions
Date: Friday, January 5, 2024 2:38:00 PM

Zahid,

If you don't mind, please allow a brief follow up to my email 1/4/2024, which asked the following question:

Would the Superintendent permit non-City employee members of the federal monitoring team and U.S. DOJ to view LEADS information in the context of their work on the consent decree involving Cleveland Police, if

(1) the members verify the same CJIS training; and

(2) US District Judge Oliver enters a protective order in the consent decree case (*United States of America v. City of Cleveland*, N.D. Ohio No. 1:15-cv-01046-SO) preventing publication of any LEADS or other confidential information?

It was pointed out to me that the monitoring team members are not really civilians in this context. *U.S. v. Puerto Rico*, 460 F.Supp.3d 159, 161, 164 (D.P.R. 2020) ("As judicial officers of an Article III court, Monitor team members are not accountable to the Commonwealth nor Department of Justice"). Thus, it may be said that they should be allowed to view unredacted records to the same extent as the presiding Judge.

I suppose the DOJ attorneys would be more like civilians in this context. This brings to mind an email exchange we had four years ago, in which it appeared that BCI deferred to the federal district court in the management of access to confidential records through the discovery process (not to overstate or mischaracterize – please see email exchange below). Of course, FRCP 5.2, as well as local rules and standing orders, may also apply, beyond any protective order.

Hopefully these additional points help round out my question from yesterday. Thank you again very much for all of your courtesy and time spent on this issue.

Respectfully,

Tim Puin

From: Zahid H. Siddiqi <Zahid.Siddiqi@ohioattorneygeneral.gov>
Sent: Wednesday, January 8, 2020 3:18 PM
To: Puin, Timothy <tpuin@city.cleveland.oh.us>
Cc: brian.bardwell@chandralaw.com; Boop, Elena <EBoop@city.cleveland.oh.us>; kmmiley@wilkersonlpa.com; Keefer, Katherine <KKeefer@city.cleveland.oh.us>; ewilkerson@wilkersonlpa.com; Kretch, Wesley <WKretch@city.cleveland.oh.us>; Pike, Michael <MPike@city.cleveland.oh.us>
Subject: RE: White v. Cleveland - 1:17-CV-1165 [IWOV-INVESTIGATION.FID215091]

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or

open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Mr. Puin-

The photo arrays that were attached to Mr. Bardwell's email contained three pages for each lineup – one identification page that identified the law enforcement officer as well as the witness viewing that lineup, one page with six photos and an ID number for each photo, and a third page with the name, weight, and height of each individual. There were also three attachments to his email that appeared to be presented to three distinct eyewitnesses. Each attachment was roughly 15 pages each. I apologize, but I deleted the email containing the attachments, so I am going off of my memory.

I won't be looped into a discovery dispute between parties in a lawsuit to which my client is not involved. The analysis is different when examining it from a public records request under R.C. 149.43 and when a subpoena is issued for the documents. OHLEG records are not a matter of public record under R.C. 109.57(D), so if the request came in that way, it would be denied. If the records were subpoenaed, those rules do not apply and we would comply with the request unless Ohio or federal law protects the records from dissemination. Because these records were never in the custody of BCI, we would not have furnished them in response to a subpoena in any event.

BCI has no dog in the fight, and this is truly a matter between the parties to the lawsuit. Best of luck working it out.

Best regards,

Zahid

From: Puin, Timothy <tpuin@city.cleveland.oh.us>

Sent: Wednesday, January 8, 2020 2:49 PM

To: Zahid H. Siddiqi <Zahid.Siddiqi@ohioattorneygeneral.gov>

Cc: brian.bardwell@chandraLaw.com; Boop, Elena <EBoop@city.cleveland.oh.us>; kmmiley@wilkersonlpa.com; Keefer, Katherine <KKeefer@city.cleveland.oh.us>; ewilkerson@wilkersonlpa.com; Kretch, Wesley <WKretch@city.cleveland.oh.us>; Pike, Michael <MPike@city.cleveland.oh.us>

Subject: RE: White v. Cleveland - 1:17-CV-1165 [IWOV-INVESTIGATION.FID215091]

Mr. Siddiqi,

Thank you. We were not copied on Brian's earlier email and so did not have the benefit of joining in that discussion.

It appears that your email refers to the photo arrays (head shots with no names or other info) and not to the photo lineup keys or OHLEG reports on victims, witnesses, suspects, etc. Is that correct? Obviously the keys and the OHLEG reports have PII, when the photo arrays per se do not.

From: [Puin, Timothy](#)
To: klocke@dps.ohio.gov; vdowdy@dps.ohio.gov
Cc: [Stone, Rick](#); [Carney, Brian](#)
Subject: R.C. 2913.04(C) request from Cleveland
Date: Thursday, January 4, 2024 5:12:00 PM

Dear Mr. Locke and Ms. Dowdy,

Cleveland Police officials suggested we contact you about seeking permission from the chair of the LEADS steering committee for certain civilian employees to view LEADS information, per R.C. 2913.04(C). If you could let us know if we've come to the right place, that would be greatly appreciated!

As background, the civilians are Public Safety-related employees including internal investigators for misconduct cases (Office of Professional Standards, Office of Integrity Control, EMS, Animal Control). They would not use LEADS data in their jobs or otherwise, but allowing them permission would remove the burden from the police and law departments of having to redact LEADS info before giving them records. The redaction process is time-consuming and delays important work.

BCI Supt. Morbitzer responded to our request re: OHLEG access for the same purposes as set forth in the email copied below.

I am happy to explain further if appropriate (there is also a question about civilians viewing LEADS info in the context of the consent decree case in court and possibly other matters).

Thank you for your courtesy and attention to this question.

Respectfully,

Tim Puin
Asst. Dir., Law Dept.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Tuesday, January 2, 2024 2:31 PM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

I spoke to the Superintendent about your request. He would like to see the members of the OPS complete CJIS security training before granting them access to view those records. It can be done online and takes between 30 minutes – one hour to complete. The training is at this link: <https://www.cjisonline.com/>. When they have completed that training, let us know and furnish verification to us and then permission will be granted.

Zahid

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: [Zahid Siddiqi](#)
To: [Puin, Timothy](#)
Cc: [Hough, Amy](#)
Subject: RE: OPS - public records requests
Date: Friday, January 5, 2024 2:41:56 PM

Tim-

I apologize, but we need to hold off on this question. There has been a change in Superintendent at BCI and he is not sure about whether he will grant access. We may be in touch with additional follow up questions about the OPS and other matters. We will meet internally and get back to you.

For your other question, BCI does not administer LEADS. That is under the Ohio State Highway Patrol's purview within the Ohio Department of Public Safety. BCI can only grant consent for OHLEG access. You would need to raise questions concerning LEADS to the Department of Public Safety.

Zahid

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Thursday, January 4, 2024 11:00 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Zahid,

My colleagues are working on rolling this out internally. We are mindful of the directive that "permission will be granted" only after verification of training is sent to BCI.

My request concerned OPS but there is a different unit also made up of City employees that also conducts internal investigations of public safety personnel, like OPS, which is known as Office of Integrity Control, Compliance, and Employee Accountability (OIC). Because its role is so similar to OPS, and its members are also City employees, we will apply the same requirements to OIC employees. Thank you again for your courtesy.

On another matter:

Would the Superintendent permit non-City employee members of the federal monitoring team and U.S. DOJ to view LEADS information in the context of their work on the consent decree involving Cleveland Police, if

(1) the members verify the same CJIS training; and

(2) US District Judge Oliver enters a protective order in the consent decree case (*United States of America v. City of Cleveland*, N.D. Ohio No. 1:15-cv-01046-SO) preventing publication of any LEADS or other confidential information?

Currently, there is a lot of redacting that goes on before records are given to the monitoring team and DOJ, which causes delays and burdens on staff. In a previous federal court case involving the City, the Superintendent permitted dissemination of OHLEG/LEADS info for purposes of the litigation subject to a protective order. I am hoping that the same logic would apply here. The parties are not completely at odds like in the previous litigation, but are working together to implement a settlement agreement under the oversight of the monitor and the court; and there would be the added protection of requiring the CJIS training.

Thank you for addressing this additional matter at your convenience. We certainly appreciate BCI's engagement in these matters.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Tuesday, January 2, 2024 2:31 PM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

I spoke to the Superintendent about your request. He would like to see the members of the OPS complete CJIS security training before granting them access to view those records. It can be done online and takes between 30 minutes – one hour to complete. The training is at this link: <https://www.cjisonline.com/>. When they have completed that training, let us know and furnish verification to us and then permission will be granted.

Zahid

From: Zahid Siddiqi
Sent: Wednesday, December 20, 2023 8:28 AM
To: 'Puin, Timothy' <tpuin@clevelandohio.gov>

Subject: RE: OPS - public records requests

Tim-

I have requested the consent of the Superintendent to disseminate the material as set forth below. When I have an opportunity to speak with him, I will pass along his position on the request.

Zahid

From: Puin, Timothy <tpuin@clevelandohio.gov>

Sent: Tuesday, December 19, 2023 11:26 AM

To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>

Subject: OPS - public records requests

Chief Counsel,

Per R.C. 2913.04(D), "No person shall knowingly gain access to, attempt to gain access to, cause access to be granted to, or disseminate information gained from access to the Ohio law enforcement gateway established and operated pursuant to division (C)(1) of section 109.57 of the Revised Code without the consent of, or beyond the scope of the express or implied consent of, the superintendent of the bureau of criminal identification and investigation."

Cleveland' Office of Professional Standards (OPS) is an independent agency within the City of Cleveland and is composed of civilians only. OPS employees are City employees and are not LEADS-certified. OPS has the responsibility of receiving and investigating non-criminal complaints filed by members of the public against sworn and non-sworn Cleveland Division of Police employees. OPS investigations require access to Internal Affairs files, dispatch audio recordings, and other records that may contain information gained from access to OHLEG/ LEADS.

Would Superintendent Morbitzer object if unredacted records were to be shared internally between the Division of Police and OPS? It is understood that OHLEG/LEADS information in any records would not be used in any OPS investigation and would not be disseminated by OPS outside the City.

Thank you for your time and attention to this matter.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi [<mailto:Zahid.Siddiqi@OhioAGO.gov>]

Sent: Monday, March 14, 2022 11:30 AM

To: Puin, Timothy <tpuin@clevelandohio.gov>; Jill Small <Jill.Small@OhioAGO.gov>

Subject: RE: OHLEG Lineup Wizard - public records requests

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Mr. Puin-

In my analysis, a prosecuting attorney would be disseminating the OHLEG output for legitimate discovery purposes within the rules of criminal procedure. This would be with the superintendent's consent and within the scope of his express or implied consent. However, I am not the superintendent, so allow me to speak with him first to learn his position on the matter.

Best regards,

Zahid



Zahid H. Siddiqi
Chief Counsel – BCI
Office of Ohio Attorney General Dave Yost
Office: 740-845-2185
Mobile: 614-264-6650
Zahid.Siddiqi@OhioAGO.gov

Confidentiality Notice: This message is intended for use only by the individual or entity to whom or which it is addressed and may contain information that is privileged, confidential and/or otherwise exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by telephone.

From: Puin, Timothy <tpuin@clevelandohio.gov>

Sent: Monday, March 14, 2022 10:33 AM

To: Jill Small <Jill.Small@OhioAGO.gov>

Cc: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>

Subject: OHLEG Lineup Wizard - public records requests

Director Small,

This email is sent per R.C. 2913.04(D), which requires the superintendent of BCI to consent to disclosures of information gained from OHLEG.

I am cc'ing BCI chief counsel, Mr. Siddiqi.

Are we allowed to turn over six-packs generated from OHLEG's Lineup Wizard application as public records, along with the lineup keys (with only PII redacted)?

Attorneys and Ohio Innocence Project have been making requests for photo lineups, which in my opinion should be disclosed. I would distinguish these from the searches run on subjects in a criminal investigation through OHLEG/LEADS, which I would see as subject to R.C. 2913.04(D).

My opinion may be mistaken, however, so I am reaching out for clarification as to whether photo lineups generated from OHLEG Lineup Wizard are public records.

Thank you for your time and attention to this matter.

Tim Puin

Timothy J. Puin
Assistant Director of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
(216) 664-2807/ Fax (216) 664-2663
tpuin@clevelandohio.gov

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: [Griffin, Mark](#)
To: [Racine, Karl](#); [Wilhelm, Abby Jae](#); [Mygatt, Timothy \(CRT\)](#); [Fitzgerald, Patricia M. \(USAOHN\)](#)
Subject: [EXTERNAL] FW: LEADS question - follow up
Date: Thursday, January 11, 2024 10:55:30 AM

FYI . . .

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Thursday, January 11, 2024 10:52 AM
To: Griffin, Mark <MGriffin@clevelandohio.gov>; Howard, Karrie <khoward2@clevelandohio.gov>; Drummond, Dornat <ddrummond@clevelandohio.gov>; Curtis, Ronda <RCurtis@clevelandohio.gov>; Butler, Geraldine <GButler@clevelandohio.gov>; Anderson, Leigh Ph.D <LAnderson2@clevelandohio.gov>; Carney, Brian <BCarney@clevelandohio.gov>; Perez, Marcus <MPerez2@clevelandohio.gov>; Stone, Rick <RStone2@clevelandohio.gov>; Moore, Daniel <DMoore@clevelandohio.gov>; Neidbalson, Charles <CNeidbalson@clevelandohio.gov>; Funari, Vincent <vfunari@clevelandohio.gov>; Fay, Daniel <DFay@clevelandohio.gov>; Todd, Dorothy <DTodd@clevelandohio.gov>; Ausbrook, Sharin <SAusbrook@clevelandohio.gov>; Sailey, Oliver Jr. <OSailey@clevelandohio.gov>; Hough, Amy <AHough@clevelandohio.gov>; Macias, Hannah <HMacias@clevelandohio.gov>; Johnson, Carlos <CJohnson2@clevelandohio.gov>
Subject: FW: LEADS question - follow up

Copied below are follow up emails re: LEADS sent to Ohio DPS today. On my calendar to follow up again next week and potentially escalate to DPS counsel if there is no response.

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Puin, Timothy
Sent: Thursday, January 11, 2024 10:44 AM
To: rabussey@dps.ohio.gov; tbrisco@dps.ohio.gov
Subject: FW: LEADS question - follow up

Sirs,

Based on Mr. Locke's out of office message, the email below is being forward to you.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Puin, Timothy
Sent: Thursday, January 11, 2024 10:41 AM
To: klocke@dps.ohio.gov; vdowdy@dps.ohio.gov
Subject: LEADS question - follow up

Good morning.

To follow up on my 1/4/2023 email, we are asking about the chair's view of LEADS data included in records that need review for purposes of police and safety personnel oversight (by Office of Professional Standards, Office of Integrity Control, Public Safety, Monitoring Team, and related entities).

The goal is more efficient sharing of records between the first-responder divisions and their oversight bodies. Currently, the redaction process is fairly time-consuming and difficult.

LEADS data would not be used for any non-law enforcement purposes, or publicized in any way. It is just incidentally included in records. Investigators conceivably could take CJIS online training (as suggested by Supt. Morbitzer of BCI) and/or sign a confidentiality pledge acceptable to DPS.

Others from the City may have contacted you and I apologize if I missed any communications.

Thanks again very much for your valuable time and attention to this inquiry, and we look forward to hearing back from you.

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: [Griffin, Mark](#)
To: [Racine, Karl](#); [Wilhelm, Abby Jae](#); [Fitzgerald, Patricia M. \(USAOHN\)](#); [Puin, Timothy](#); [Mygatt, Timothy \(CRT\)](#); [Thomas, Delante](#); [Anderson, Leigh Ph.D](#)
Subject: [EXTERNAL] Additional Email from BCI
Date: Monday, January 15, 2024 9:36:03 AM
Attachments: [RE OPS - public records requests.pdf](#)

From: [Puin, Timothy](#)
To: [Zahid Siddiqi](#)
Cc: [Hough, Amy](#)
Subject: RE: OPS - public records requests
Date: Friday, January 12, 2024 11:18:00 AM

Zahid,

Thank you to you, the Superintendent, and all concerned, for the time and attention to this inquiry. I will forward your response to the officials involved here in Cleveland and follow up with you if they wish to discuss further.

Respectfully,

Tim

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Friday, January 12, 2024 11:07 AM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

After an internal meeting and review of the OHLEG Rules and Regulations (Regulations), the Superintendent does not believe he can grant consent to the City for the Office of Professional Standards (OPS) to access OHLEG records and materials. When examining the Regulations, a few sections stand out to us in our analysis.

The Regulations define a criminal justice agency as "The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included." Page 4. The definitions also define law enforcement agency as "A police department, the office of a sheriff, the state highway patrol, a county prosecuting attorney, or a federal, state, or local governmental body that enforces criminal laws and has employees who have a statutory power of

arrest.” Page 5. Absent from these definitions is a civilian review board such as the OPS. In addition, the OPS lacks the statutory authority to arrest and does not allocate a substantial part of its budget to the administration of criminal justice.

When examining other provisions, we noted the definition of secondary dissemination, defined as “The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.” Page 8. We are not convinced that OPS is an authorized recipient agency due to it being neither a criminal justice agency nor a law enforcement agency. This is supported by Regulation 4.0, which reads:

CJI shall only be used and disseminated consistent with the authorized purpose for which it was accessed. Dissemination of CJI to another agency is authorized if (a) the other agency is an authorized recipient of such information, or (b) the other agency is performing personnel and appointment functions with codified authority to obtain CJI for criminal justice employment applicants.

Regulation 4.0, Page 24. Based on our understanding of OPS’ mission, we do not feel that OPS fits that definition.

If you can share more information about OPS and its mission, we can discuss further. But as it currently stands, we don’t feel the Regulations authorize the dissemination of OHLEG materials to the OPS.

Feel free to reach out should you have questions or concerns.

Respectfully,

Zahid



Zahid H. Siddiqi
Chief Counsel – BCI
Office of Ohio Attorney General Dave Yost
1560 S.R. 56 S.W.
London, OH 43140
Office: 740-845-2185
Mobile: 614-264-6650
Zahid.Siddiqi@OhioAGO.gov

Confidentiality Notice: This message is intended for use only by the individual or entity to whom or which it is addressed and may contain information that is privileged, confidential and/or otherwise exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by telephone.

From: Puin, Timothy <tpuin@clevelandohio.gov>

Sent: Friday, January 5, 2024 2:43 PM

To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Understood, thank you sir!

We will follow up but your time is greatly appreciated.

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Friday, January 5, 2024 2:42 PM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

I apologize, but we need to hold off on this question. There has been a change in Superintendent at BCI and he is not sure about whether he will grant access. We may be in touch with additional follow up questions about the OPS and other matters. We will meet internally and get back to you.

For your other question, BCI does not administer LEADS. That is under the Ohio State Highway Patrol's purview within the Ohio Department of Public Safety. BCI can only grant consent for OHLEG access. You would need to raise questions concerning LEADS to the Department of Public Safety.

Zahid

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Thursday, January 4, 2024 11:00 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Zahid,

My colleagues are working on rolling this out internally. We are mindful of the directive that

“permission will be granted” only after verification of training is sent to BCI.

My request concerned OPS but there is a different unit also made up of City employees that also conducts internal investigations of public safety personnel, like OPS, which is known as Office of Integrity Control, Compliance, and Employee Accountability (OIC). Because its role is so similar to OPS, and its members are also City employees, we will apply the same requirements to OIC employees. Thank you again for your courtesy.

On another matter:

Would the Superintendent permit non-City employee members of the federal monitoring team and U.S. DOJ to view LEADS information in the context of their work on the consent decree involving Cleveland Police, if

(1) the members verify the same CJIS training; and

(2) US District Judge Oliver enters a protective order in the consent decree case (*United States of America v. City of Cleveland*, N.D. Ohio No. 1:15-cv-01046-SO) preventing publication of any LEADS or other confidential information?

Currently, there is a lot of redacting that goes on before records are given to the monitoring team and DOJ, which causes delays and burdens on staff. In a previous federal court case involving the City, the Superintendent permitted dissemination of OHLEG/LEADS info for purposes of the litigation subject to a protective order. I am hoping that the same logic would apply here. The parties are not completely at odds like in the previous litigation, but are working together to implement a settlement agreement under the oversight of the monitor and the court; and there would be the added protection of requiring the CJIS training.

Thank you for addressing this additional matter at your convenience. We certainly appreciate BCI's engagement in these matters.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Tuesday, January 2, 2024 2:31 PM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

I spoke to the Superintendent about your request. He would like to see the members of the OPS complete CJIS security training before granting them access to view those records. It can be done online and takes between 30 minutes – one hour to complete. The training is at this link: <https://www.cjisonline.com/>. When they have completed that training, let us know and furnish verification to us and then permission will be granted.

Zahid

From: Zahid Siddiqi
Sent: Wednesday, December 20, 2023 8:28 AM
To: 'Puin, Timothy' <tpuin@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

I have requested the consent of the Superintendent to disseminate the material as set forth below. When I have an opportunity to speak with him, I will pass along his position on the request.

Zahid

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Tuesday, December 19, 2023 11:26 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Subject: OPS - public records requests

Chief Counsel,

Per R.C. 2913.04(D), “No person shall knowingly gain access to, attempt to gain access to, cause access to be granted to, or disseminate information gained from access to the Ohio law enforcement gateway established and operated pursuant to division (C)(1) of section 109.57 of the Revised Code without the consent of, or beyond the scope of the express or implied consent of, the superintendent of the bureau of criminal identification and investigation.”

Cleveland’ Office of Professional Standards (OPS) is an independent agency within the City of Cleveland and is composed of civilians only. OPS employees are City employees and are not LEADS-certified. OPS has the responsibility of receiving and investigating non-criminal complaints filed by

members of the public against sworn and non-sworn Cleveland Division of Police employees. OPS investigations require access to Internal Affairs files, dispatch audio recordings, and other records that may contain information gained from access to OHLEG/ LEADS.

Would Superintendent Morbitzer object if unredacted records were to be shared internally between the Division of Police and OPS? It is understood that OHLEG/LEADS information in any records would not be used in any OPS investigation and would not be disseminated by OPS outside the City.

Thank you for your time and attention to this matter.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi [<mailto:Zahid.Siddiqi@OhioAGO.gov>]

Sent: Monday, March 14, 2022 11:30 AM

To: Puin, Timothy <tpuin@clevelandohio.gov>; Jill Small <Jill.Small@OhioAGO.gov>

Subject: RE: OHLEG Lineup Wizard - public records requests

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Mr. Puin-

In my analysis, a prosecuting attorney would be disseminating the OHLEG output for legitimate discovery purposes within the rules of criminal procedure. This would be with the superintendent's consent and within the scope of his express or implied consent. However, I am not the superintendent, so allow me to speak with him first to learn his position on the matter.

Best regards,

Zahid



Zahid H. Siddiqi
Chief Counsel – BCI
Office of Ohio Attorney General Dave Yost
Office: 740-845-2185
Mobile: 614-264-6650
Zahid.Siddiqi@OhioAGO.gov

Confidentiality Notice: This message is intended for use only by the individual or entity to whom or which it is addressed and may contain information that is privileged, confidential and/or otherwise exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by telephone.

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Monday, March 14, 2022 10:33 AM
To: Jill Small <Jill.Small@OhioAGO.gov>
Cc: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Subject: OHLEG Lineup Wizard - public records requests

Director Small,

This email is sent per R.C. 2913.04(D), which requires the superintendent of BCI to consent to disclosures of information gained from OHLEG.

I am cc'ing BCI chief counsel, Mr. Siddiqi.

Are we allowed to turn over six-packs generated from OHLEG's Lineup Wizard application as public records, along with the lineup keys (with only PII redacted)?

Attorneys and Ohio Innocence Project have been making requests for photo lineups, which in my opinion should be disclosed. I would distinguish these from the searches run on subjects in a criminal investigation through OHLEG/LEADS, which I would see as subject to R.C. 2913.04(D).

My opinion may be mistaken, however, so I am reaching out for clarification as to whether photo lineups generated from OHLEG Lineup Wizard are public records.

Thank you for your time and attention to this matter.

Tim Puin

Timothy J. Puin
Assistant Director of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077

(216) 664-2807/ Fax (216) 664-2663
tpuin@clevelandohio.gov

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: [Anderson, Leigh Ph.D](#)
To: [Christine Cole](#); [Heyer, Michelle L. \(USAOHN\)](#); [Evanovich, Michael \(USAOHN\) \[Contractor\]](#); [DeCaro, Sara \(USAOHN\)](#); [Geissler, Jonas \(CRT\)](#); [Coromelas, Acrivi \(CRT\)](#); [karl.racine@hoganlovells.com](#); [Wilhelm, Abby Jae](#); [Lisa Fink](#); [Caruso, Courtney](#); [Yonekura, Stephanie](#); ["Rick Myers"](#); [Shunta Boston](#); [Fitzgerald, Patricia M. \(USAOHN\)](#); [Mygatt, Timothy \(CRT\)](#)
Cc: [Macias, Hannah](#); [Johnson, Carlos](#); [Griffin, Mark](#); [Thomas, Delante](#); [Humphrey, Joyce L](#); [Carney, Brian](#); [Dye, Jakimah](#); [Todd, Dorothy](#); [Drummond, Dornat](#); [Simon, Robert](#); [Butler, Geraldine](#); [Howard, Karrie](#); [Fischbach, Tiffany](#); [Puin, Timothy](#); [Menzalora, William](#); [Pillow, Ali](#); [Morris, Sammy](#); [Fay, Daniel](#); [Maguth, Mark](#); [Stone, Rick](#)
Subject: [EXTERNAL] UPDATE: LEADS Access
Date: Tuesday, February 6, 2024 2:55:11 PM
Attachments: [Outlook-jallnrb.png](#)
[Cleveland LEADS Access Letter \(003\).pdf](#)
Importance: High

Greetings All,

Please see the attached letter from the Acting LEADS Administrator, Victoria Dowdy.

The City looks forward to further discussing the matter.

Many thanks!

In Truth and Service,



Leigh R. Anderson, PhD., MPA-IG, CIGA, CIGE
Executive Director
Police Accountability Team
City of Cleveland, Ohio
Desk Phone: 216-664-2951
Email: landerson2@clevelandohio.gov

"In any moment of decision, the best thing you can do is the right thing, the next best thing you can do is the wrong thing, and the worst thing you can do is nothing." -Theodore Roosevelt



LEADS STEERING COMMITTEE

- Sheriff Randy Thorp
- Judge Beth W. Cappelli
- Superintendent Joe Morbitzer
- Chief Vincent Molnar
- Captain Dennis Swingley
- Sheriff Matthew Hafey
- Chief Gary D. Lewis, Jr.

Major Matthew Them, Chair, LEADS Steering Committee

February 2, 2024

Cleveland Division of Police
Acting Lieutenant Rick Stone
2001 Payne Avenue
Cleveland, Ohio 44114

Dear Acting Lt. Stone:

LEADS has denied the request to permit civilian public safety employees to review Criminal Justice Information (CJI) since they are not authorized recipients and the purpose does not qualify as the administration of criminal justice.

Per LEADS Administrative Rule 4501:2-10-01 Definitions (A): "Administration of criminal justice" means the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

Per LEADS Administrative Rule 4501:2-10-06 Dissemination and Record Keeping (C): Messages and/or throughput of any kind accessed through LEADS shall be restricted to the use of duly authorized law enforcement and/or criminal justice agencies for the administration of criminal justice.

You can reference the LEADS Administrative Rules and the FBI CJIS Security Policy further at www.leads.ohio.gov.

If you have any further questions, please don't hesitate to contact me at 614-420-4737 or vdowdy@dps.ohio.gov.

Sincerely,

A handwritten signature in cursive script that reads "Victoria Dowdy".

Victoria Dowdy
Acting LEADS Administrator

From: [Griffin, Mark](#)
To: vdowdy@dps.ohio.gov
Cc: [Racine, Karl](#); [Wilhelm, Abby Jae](#); [Mygatt, Timothy \(CRT\)](#); [Fitzgerald, Patricia M. \(USAOHN\)](#)
Subject: [EXTERNAL] Request for Clarification Regarding LEADS Access
Date: Thursday, February 15, 2024 10:19:00 AM
Attachments: [LEADS Administrator Letter - PDF.pdf](#)

February 15, 2024

Ms. Victoria Dowdy
Acting LEADS Administrator
1970 West Broad Street
P.O. Box 182075
Columbus, Ohio 43218-2075

Re: LEADS Access for Court Monitoring Team and Department of Justice, Civil Rights Division

Dear Administrator Dowdy,

The City of Cleveland seeks clarification regarding whether access to protected information contained within Cleveland Division of Police (“CDP”) documents and databases by the Monitoring Team appointed by the U.S. District Court for the Northern District of Ohio (“Monitoring Team”) and the Department of Justice, Civil Rights Division (“DOJ”) complies with Ohio state law. To the extent necessary, the City requests that the chair of the law enforcement automated data system (“LEADS”) steering committee, or their designee, give consent for and the Monitoring Team and DOJ to have such access.

On June 12, 2015, the United States District Court for the Northern District of Ohio (“Court”), approved a Settlement Agreement between the Parties addressing issues of constitutional policing by CDP. The Court also appointed a Monitor to assist the Court, the Parties, and the Cleveland community in assessing compliance with the court-ordered Settlement Agreement. The Monitor supervises a Monitoring Team that evaluates implementation and compliance with the Settlement Agreement, provides technical assistance, and issues public reports on the City’s compliance with the Agreement. The Monitor reports to the Court and is an agent of the Court. Settlement Agreement, ¶ 351. The Settlement Agreement requires the City and CDP to give the Monitor and DOJ “full and direct access to all City and CDP documents and data related to the Agreement.” Settlement Agreement, ¶

390; see also ¶¶ 389, 391. The Settlement Agreement obligates the Monitor and DOJ to “maintain all confidential or non-public information provided by the City and CDP in a confidential manner.” Settlement Agreement, ¶ 395.

To evaluate implementation and compliance, the Monitoring Team conducts a variety of assessments. To conduct these assessments, the Monitoring Team reviews CDP reports, documents, and data, such as body-worn camera footage; incident reports; use of force reports; taser deployment information; stop, search, and arrest reports; supervisor review of stop, search, arrest, and use of force reports; complaints; IAPro files; and CJJ. DOJ also reviews these documents to independently verify the Monitoring Team’s assessments and to evaluate the City’s compliance with the Settlement Agreement.

Until recently, the City has given the Monitoring Team and DOJ access to CDP documents and CJJ databases as required by the Settlement Agreement, including IAPro, Blue Team, Evidence.com, Brazos, and CDP’s Records Management System. Neither the Monitoring Team nor DOJ sought to review criminal history, personal identifying information, or any other LEADS data, because those are not necessary to their review, but some of the documents and records may have incidentally contained such information. Instead, the Monitoring Team and DOJ only seek to review data gathered by CDP that CDP enters and tracks through LEADS and CJIS. For example, since 2018, the Monitoring Team has conducted assessments of use of force incidents. *See United States v. City of Cleveland*, Case No. 15cv1046, ECF No. 333 (Oct. 31, 2020 N.D. Ohio) (describing the methodology and explaining that the City will be providing case files through Box). Previously, the City has provided complete Use of Force case files to the Monitoring Team and DOJ, which including access to IAPro, Blue Team, Law Enforcement Records Management System (LERMS), Brazos Software, Field Base Reporting (FBR) and Evidence.com. Similarly, since 2020, the Monitoring Team has conducted assessments of the Civilian Police Review Board. To do so, the Monitoring Team and DOJ had access to IAPro, LERMS and Evidence.com. *Id.* Likewise, since 2020, the Monitoring Team has conducted assessments of CDP’s Force Review Board, which required the review of all materials sent to the Force Review Board and to attend its

meetings. *Id.* Before these meetings, the City has provided the Monitoring Team and DOJ with relevant files from IAPro, LERMS, FBR, Blue Team, and Evidence.com. And the Monitoring Team has been working with CDP to conduct a search and seizure assessment, which in addition to those systems will require access to Brazos.

On December 29, 2023, the City paused DOJ and Monitoring Team access to Field Base Reporting (FBR), LERMS, LEADS, and evidence.com. The City informed DOJ and the Monitoring Team that the City was required to limit access to CDP documents and data pursuant to Ohio law, and in particular the Ohio Law Enforcement Automated Data System law, O.A.C. 4501-2-10-01 *et seq.* and R.C. 2913.04. The City has informed DOJ and the Monitoring Team that Ohio LEADS limits their access to CDP's databases, including Evidence.com, IAPro, Blue Team, Brazos, and LERMS. Accordingly, the Monitoring Team and DOJ no longer have access to body-worn camera footage; incident reports; use of force reports; taser deployment information; stop, search, and arrest reports; supervisor review of stop, search, arrest, and use of force reports; complaints; and IAPro files. The Monitoring Team and DOJ are unable to conduct their compliance assessments without access to these files and systems.

The City seeks an opinion from the Chair of the Leads Steering Committee, or their designee, in clarifying that the City and CDP would not be violating Ohio law if the City resumes giving the Monitoring Team and DOJ unredacted access to the above-described documents and records, which also include LEADS and CJIS information. These records are necessary for the Monitoring Team to assess compliance with the Settlement Agreement and to fulfil its duties as an agent of the court, and for DOJ to verify compliance with the Decree. Access to these documents is consistent with the Ohio definition of a "criminal justice agency" because the Monitoring Team is an arm of a court and DOJ arguably performs the administration of criminal justice. Accordingly, we believe that the Monitoring Team and DOJ can access CJIS information that would otherwise be protected under Ohio law. See Ohio Administrative Code § 4501:2-10-01(I). We therefore believe the City can provide these unredacted documents to the Monitoring Team and DOJ pursuant to Ohio law. Please confirm

that our interpretation of Ohio law is correct. We note that the definition of a “criminal justice agency” is identical to that found in the federal Criminal Justice Information Systems (“CJIS”) regulations, see 28 C.F.R. § 20.3(g), and DOJ regularly has access to these documents and records in its investigations and cases across the country, including those that may incidentally contain CJIS information.

To the extent necessary, the City further seeks consent from the chair of the law enforcement automated data system steering committee for the Monitoring Team and DOJ to have CJIS access as provided in R.C. 2913.04. If you conclude that a court order or protective order beyond the protection already provided in the Settlement Agreement is necessary for the Monitoring Team and DOJ to have access, please let us know as soon as possible, including any criteria you believe must be included in the order.

Best Regards,

Mark Griffin

Law Director & Chief Legal Counsel

City of Cleveland

CC: Karl Racine, Stephanie Yonekura, Abby Wilhelm, Monitoring Team
Patricia Fitzgerald, Tim Mygatt, Department of Justice



City of Cleveland

Justin M. Bibb, Mayor

Department of Law

Mark Griffin, Director

601 Lakeside Avenue, Room 106

Cleveland, Ohio 44114-1077

216/664-2800 – Fax: 216/664-2663

www.cleveland.oh.gov

February 15, 2024

Ms. Victoria Dowdy
Acting LEADS Administrator
1970 West Broad Street
P.O. Box 182075
Columbus, Ohio 43218-2075

Re: LEADS Access for Court Monitoring Team and Department of Justice,
Civil Rights Division

Dear Administrator Dowdy,

The City of Cleveland seeks clarification regarding whether access to protected information contained within Cleveland Division of Police (“CDP”) documents and databases by the Monitoring Team appointed by the U.S. District Court for the Northern District of Ohio (“Monitoring Team”) and the Department of Justice, Civil Rights Division (“DOJ”) complies with Ohio state law. To the extent necessary, the City requests that the chair of the law enforcement automated data system (“LEADS”) steering committee, or their designee, give consent for and the Monitoring Team and DOJ to have such access.

On June 12, 2015, the United States District Court for the Northern District of Ohio (“Court”), approved a Settlement Agreement between the Parties addressing issues of constitutional policing by CDP. The Court also appointed a Monitor to assist the

Court, the Parties, and the Cleveland community in assessing compliance with the court-ordered Settlement Agreement. The Monitor supervises a Monitoring Team that evaluates implementation and compliance with the Settlement Agreement, provides technical assistance, and issues public reports on the City's compliance with the Agreement. The Monitor reports to the Court and is an agent of the Court. Settlement Agreement, ¶ 351. The Settlement Agreement requires the City and CDP to give the Monitor and DOJ "full and direct access to all City and CDP documents and data related to the Agreement." Settlement Agreement, ¶ 390; see also ¶¶ 389, 391. The Settlement Agreement obligates the Monitor and DOJ to "maintain all confidential or non-public information provided by the City and CDP in a confidential manner." Settlement Agreement, ¶ 395.

To evaluate implementation and compliance, the Monitoring Team conducts a variety of assessments. To conduct these assessments, the Monitoring Team reviews CDP reports, documents, and data, such as body-worn camera footage; incident reports; use of force reports; taser deployment information; stop, search, and arrest reports; supervisor review of stop, search, arrest, and use of force reports; complaints; IAPro files; and CJI. DOJ also reviews these documents to independently verify the Monitoring Team's assessments and to evaluate the City's compliance with the Settlement Agreement.

Until recently, the City has given the Monitoring Team and DOJ access to CDP documents and CJI databases as required by the Settlement Agreement, including IAPro, Blue Team, Evidence.com, Brazos, and CDP's Records Management System. Neither the Monitoring Team nor DOJ sought to review criminal history, personal identifying information, or any other LEADS data, because those are not necessary to their review, but some of the documents and records may have incidentally contained such

Page 3 of 5

information. Instead, the Monitoring Team and DOJ only seek to review data gathered by CDP that CDP enters and tracks through LEADS and CJIS. For example, since 2018, the Monitoring Team has conducted assessments of use of force incidents. *See United States v. City of Cleveland*, Case No. 15cv1046, ECF No. 333 (Oct. 31, 2020 N.D. Ohio) (describing the methodology and explaining that the City will be providing case files through Box). Previously, the City has provided complete Use of Force case files to the Monitoring Team and DOJ, which including access to IAPro, Blue Team, Law Enforcement Records Management System (LERMS), Brazos Software, Field Base Reporting (FBR) and Evidence.com. Similarly, since 2020, the Monitoring Team has conducted assessments of the Civilian Police Review Board. To do so, the Monitoring Team and DOJ had access to IAPro, LERMS and Evidence.com. *Id.* Likewise, since 2020, the Monitoring Team has conducted assessments of CDP's Force Review Board, which required the review of all materials sent to the Force Review Board and to attend its meetings. *Id.* Before these meetings, the City has provided the Monitoring Team and DOJ with relevant files from IAPro, LERMS, FBR, Blue Team, and Evidence.com. And the Monitoring Team has been working with CDP to conduct a search and seizure assessment, which in addition to those systems will require access to Brazos.

On December 29, 2023, the City paused DOJ and Monitoring Team access to Field Base Reporting (FBR), LERMS, LEADS, and evidence.com. The City informed DOJ and the Monitoring Team that the City was required to limit access to CDP documents and data pursuant to Ohio law, and in particular the Ohio Law Enforcement Automated Data System law, O.A.C. 4501-2-10-01 *et seq.* and R.C. 2913.04. The City has informed DOJ and the Monitoring Team that Ohio LEADS limits their access to CDP's databases, including Evidence.com, IAPro, Blue Team, Brazos, and LERMS

Page 4 of 5

Accordingly, the Monitoring Team and DOJ no longer have access to body-worn camera footage; incident reports; use of force reports; taser deployment information; stop, search, and arrest reports; supervisor review of stop, search, arrest, and use of force reports; complaints; and IAPro files. The Monitoring Team and DOJ are unable to conduct their compliance assessments without access to these files and systems.

The City seeks an opinion from the Chair of the Leads Steering Committee, or their designee, in clarifying that the City and CDP would not be violating Ohio law if the City resumes giving the Monitoring Team and DOJ unredacted access to the above-described documents and records, which also include LEADS and CJIS information. These records are necessary for the Monitoring Team to assess compliance with the Settlement Agreement and to fulfil its duties as an agent of the court, and for DOJ to verify compliance with the Decree. Access to these documents is consistent with the Ohio definition of a “criminal justice agency” because the Monitoring Team is an arm of a court and DOJ arguably performs the administration of criminal justice. Accordingly, we believe that the Monitoring Team and DOJ can access CJIS information that would otherwise be protected under Ohio law. See Ohio Administrative Code § 4501:2-10-01(I). We therefore believe the City can provide these un-redacted documents to the Monitoring Team and DOJ pursuant to Ohio law. Please confirm that our interpretation of Ohio law is correct. We note that the definition of a “criminal justice agency” is identical to that found in the federal Criminal Justice Information Systems (“CJIS”) regulations, see 28 C.F.R. § 20.3(g), and DOJ regularly has access to these documents and records in its investigations and cases across the country, including those that may incidentally contain CJIS information.

Page 5 of 5

To the extent necessary, the City further seeks consent from the chair of the law enforcement automated data system steering committee for the Monitoring Team and DOJ to have CJIS access as provided in R.C. 2913.04. If you conclude that a court order or protective order beyond the protection already provided in the Settlement Agreement is necessary for the Monitoring Team and DOJ to have access, please let us know as soon as possible, including any criteria you believe must be included in the order.

Best Regards,

A handwritten signature in blue ink, appearing to read "M. D. J. A.", is positioned above the typed name and title.

Law Director & Chief Legal Counsel

City of Cleveland

CC: Karl Racine, Stephanie Yonekura, Abby Wilhelm, Monitoring Team
Patricia Fitzgerald, Tim Mygatt, Department of Justice

From: [Griffin, Mark](#)
To: [Racine, Karl](#); [Wilhelm, Abby Jae](#); [Mygatt, Timothy \(CRT\)](#); [Fitzgerald, Patricia M. \(USAOHN\)](#)
Cc: [Thomas, Delante](#); [Anderson, Leigh](#); [Johnson, Carlos](#); [Macias, Hannah](#); [Puin, Timothy](#)
Subject: [EXTERNAL] MT's Request for Emails re: LEADS Access
Date: Wednesday, February 28, 2024 5:15:02 PM
Attachments: [LEADS-access communications.pdf](#)

I asked my staff and CDP to provide “all communications with the State of Ohio regarding access to LEADS by the MT, DOJ, OPS or other oversight entities. Further, if you have similar emails with FBI/DOJ regarding LEADS Access, please also provide those.”

They provided the attached document.

The communications are set forth chronologically.

From: KJHall@dps.ohio.gov
To: [Stone, Rick](#)
Subject: RE: [EXTERNAL]OPS agreement
Date: Tuesday, May 16, 2023 2:39:05 PM
Attachments: [image001.png](#)

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Rick,

Here is the pertinent section that defines what the "Administration of criminal justice" is. It does not sound like this review board has anything to do with these functions.

From the LEADS Administrative Rules, section 4501:10-01:

(A) "Administration of criminal justice" means the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in "Neighborhood Watch" or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

My supervisor Kevin Locke will be drafting an email with the decision that this group does not meet the Administration of criminal justice guidelines.

Thanks!

Kris Hall
Infrastructure Specialist 1
LEADS Security
Ohio State Highway Patrol
1970 West Broad Street Columbus OH 43223
614.387.5424
kjhall@dps.ohio.gov



From: Stone, Rick <RStone2@clevelandohio.gov>

Sent: Tuesday, May 16, 2023 8:41 AM

To: Hall, Kris <KJHall@dps.ohio.gov>

Subject: [EXTERNAL]OPS agreement

Kris,

Good Morning.

At your earliest convenience can you call me to discuss what agreement is need for OPS?

Thanks

Rick Stone, Sergeant #9253
Cleveland Division of Police
LEADS Unit & TIU OIC / TAC
2001 Payne Ave.
Cleveland Ohio, 44114
(216) 623-2122 - Office
(216) 272-2716 - Cell
Rstone2@ClevelandOhio.gov



CAUTION: This email was received from an EXTERNAL source, use caution when clicking links or opening attachments.
If you believe this to be a malicious and/or phishing email, please send this email as an attachment to ServiceDesk@dps.ohio.gov.

From: KLocke@dps.ohio.gov
To: [Stone, Rick](#)
Subject: Cleveland Office of Professional Standards
Date: Tuesday, May 23, 2023 10:22:33 AM
Attachments: [image001.png](#)

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Morning Sgt. Stone,

Please give me a call when you are available.

Thanks

Kevin J. Locke
Information Security Officer (ISO)
LEADS Security Supervisor
Ohio State Highway Patrol
1970 West Broad Street
Columbus, Ohio 43223
[\(614\) 466-3055](tel:(614)466-3055) Help Desk
[\(614\) 387-6156](tel:(614)387-6156) Direct
[\(614\) 644-2459](tel:(614)644-2459) FAX



From: KLocke@dps.ohio.gov <KLocke@dps.ohio.gov>

Sent: Wednesday, August 2, 2023 8:31 AM

To: Stone, Rick <RStone2@clevelandohio.gov>

Subject: RE: [EXTERNAL]RE: LEADS Access

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Hi Rick,

1300 works.

Thanks

Kevin J. Locke
Information Security Officer (ISO)
LEADS Security Supervisor
Ohio State Highway Patrol
1970 West Broad Street
Columbus, Ohio 43223
(614) 466-3055 Help Desk
(614) 387-6156 Direct
(614) 644-2459 FAX



From: Stone, Rick <RStone2@clevelandohio.gov>

Sent: Wednesday, August 2, 2023 8:29 AM

To: Maguth, Mark <MMaguth@clevelandohio.gov>; Simon, Robert <rsimon@clevelandohio.gov>;
Locke, Kevin <KLocke@dps.ohio.gov>

Subject: [EXTERNAL]RE: LEADS Access

Kevin,

Would 1300 work today?

Respectfully,

Rick Stone, Sergeant #9253
Cleveland Division of Police
LEADS Unit & TIU OIC / TAC

Sent: Wednesday, August 2, 2023 8:40 AM

To: Locke, Kevin <KLocke@dps.ohio.gov>

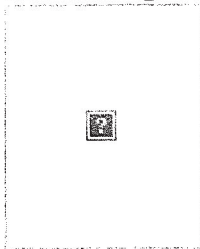
Subject: RE: [EXTERNAL]RE: LEADS Access

Great.

Do you prefer just a phone call on speaker or an invite with a dial-in code? Also, is there another number to call you at? The number listed says it's not in-service.

Thanks

Rick Stone, Sergeant #9253
Cleveland Division of Police
LEADS Unit & TIU OIC / TAC
2001 Payne Ave.
Cleveland Ohio, 44114
(216) 623-2122 - Office
(216) 272-2716 - Cell
Rstone2@ClevelandOhio.gov



From: KLocke@dps.ohio.gov <KLocke@dps.ohio.gov>

Sent: Wednesday, August 2, 2023 8:46 AM

To: Stone, Rick <RStone2@clevelandohio.gov>

Subject: RE: [EXTERNAL]RE: LEADS Access

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Hi Rick,

Can you schedule it in TEAMS?

My direct number is 614-387-6156.

Thanks

Kevin J. Locke
Information Security Officer (ISO)
LEADS Security Supervisor
Ohio State Highway Patrol
1970 West Broad Street
Columbus, Ohio 43223
(614) 466-3055 Help Desk
(614) 387-6156 Direct
(614) 644-2459 FAX



From: Maguth, Mark
To: Simon, Robert; Stone, Rick; "KLocke@dps.ohio.gov"
Subject: LEADS Discussion

Microsoft Teams meeting

Join on your computer, mobile app or room device

Click here to join the meeting <https://teams.microsoft.com/l/meetup-join/19%3ameeting_YjQ5Y2U5YTgtOTk4Ny00ZjdjLThhZGYtNTlhMDZlZTJjMTQ1%40thread.v2/0?context=%7b%22Tid%22%3a%2276e2f963-8a1d-45bf-8e06-87a368508b40%22%2c%22Oid%22%3a%22c85bae8d-b618-4e5b-8323-23c20a03c0a1%22%7d%7d>

Meeting ID: 282 304 958 517

Passcode: 4em7Bh

Download Teams <<https://www.microsoft.com/en-us/microsoft-teams/download-app>> | Join on the web <<https://www.microsoft.com/microsoft-teams/join-a-meeting>>

Or call in (audio only)

+1 216-306-2628,,916381282# <tel:+12163062628,,916381282> United States, Cleveland

Phone Conference ID: 916 381 282#

Find a local number <<https://dialin.teams.microsoft.com/e4c8bb17-f4d0-444a-b567-7d5bb2ab205c?id=916381282>> | Reset PIN

<<https://dialin.teams.microsoft.com/usp/pstnconferencing>>

Learn More <<https://aka.ms/JoinTeamsMeeting>> | Meeting options <https://teams.microsoft.com/meetingOptions/?organizerId=c85bae8d-b618-4e5b-8323-23c20a03c0a1&tenantId=76e2f963-8a1d-45bf-8e06-87a368508b40&threadId=19_meeting_YjQ5Y2U5YTgtOTk4Ny00ZjdjLThhZGYtNTlhMDZlZTJjMTQ1@thread.v2&messageId=0&language=en-US>

US>

From: KLocke@dps.ohio.gov
To: [Stone, Rick](#); [Maguth, Mark](#); [Simon, Robert](#)
Cc: cwbarrett@dps.ohio.gov; KLocke@dps.ohio.gov; TBrisco@dps.ohio.gov
Subject: RE: [EXTERNAL]RE: LEADS Access
Date: Wednesday, August 2, 2023 3:46:42 PM
Attachments: [image001.png](#)
[image004.png](#)

CAUTION: This email originated from outside of the City of Cleveland. Do not click on links or open attachments unless you recognize the sender and know that the content is safe. If you believe that this email is suspicious, please forward to phishing@clevelandohio.gov.

Afternoon Gentlemen,

The following email was sent by the FBI.

Kevin/Casey,

They do not fall under the definition of the administration of criminal justice. This would also apply to the US DOJ.

Essentially what I stated on the call, just in different and more exact terms.

So the escort option and document redaction would be ways to move forward.

Hope this helps. Let me know if you guys have additional questions.

Jeff

Jeff Campbell, CISSP

Deputy Information Security Officer
FBI/CJIS Division/CIAU/ISO Program Office
1000 Custer Hollow Rd.
Clarksburg, WV 26306
304.625.4961 (office / fax) | 304.476.4711 (mobile)
<https://le.fbi.gov/cjis-division-resources/cjis-security-policy-resource-center>

Kevin J. Locke
Information Security Officer (ISO)
LEADS Security Supervisor
Ohio State Highway Patrol
1970 West Broad Street
Columbus, Ohio 43223
(614) 466-3055 Help Desk
(614) 387-6156 Direct
(614) 644-2459 FAX



From: Tim J. Puin <tim.puin@ohioleg.gov>
Sent: Tuesday, December 19, 2023 11:26 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Subject: OPS - public records requests

Chief Counsel,

Per R.C. 2913.04(D), "No person shall knowingly gain access to, attempt to gain access to, cause access to be granted to, or disseminate information gained from access to the Ohio law enforcement gateway established and operated pursuant to division (C)(1) of section 109.57 of the Revised Code without the consent of, or beyond the scope of the express or implied consent of, the superintendent of the bureau of criminal identification and investigation."

Cleveland' Office of Professional Standards (OPS) is an independent agency within the City of Cleveland and is composed of civilians only. OPS employees are City employees and are not LEADS-certified. OPS has the responsibility of receiving and investigating non-criminal complaints filed by members of the public against sworn and non-sworn Cleveland Division of Police employees. OPS investigations require access to Internal Affairs files, dispatch audio recordings, and other records that may contain information gained from access to OHLEG/ LEADS.

Would Superintendent Morbitzer object if unredacted records were to be shared internally between the Division of Police and OPS? It is understood that OHLEG/LEADS information in any records would not be used in any OPS investigation and would not be disseminated by OPS outside the City.

Thank you for your time and attention to this matter.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

From: Zahid Siddiqi

Sent: Wednesday, December 20, 2023 8:28 AM

To: 'Puin, Timothy' <tpuin@clevelandohio.gov>

Subject: RE: OPS - public records requests

Tim-

I have requested the consent of the Superintendent to disseminate the material as set forth below. When I have an opportunity to speak with him, I will pass along his position on the request.

Zahid

From: Puin, Timothy
To: klocke@dps.ohio.gov; vdowdy@dps.ohio.gov
Cc: Stone, Rick; Carney, Brian
Subject: R.C. 2913.04(C) request from Cleveland
Date: Thursday, January 4, 2024 5:12:00 PM

Dear Mr. Locke and Ms. Dowdy,

Cleveland Police officials suggested we contact you about seeking permission from the chair of the LEADS steering committee for certain civilian employees to view LEADS information, per R.C. 2913.04(C). If you could let us know if we've come to the right place, that would be greatly appreciated!

As background, the civilians are Public Safety-related employees including internal investigators for misconduct cases (Office of Professional Standards, Office of Integrity Control, EMS, Animal Control). They would not use LEADS data in their jobs or otherwise, but allowing them permission would remove the burden from the police and law departments of having to redact LEADS info before giving them records. The redaction process is time-consuming and delays important work.

BCI Supt. Morbitzer responded to our request re: OHLEG access for the same purposes as set forth in the email copied below.

I am happy to explain further if appropriate (there is also a question about civilians viewing LEADS info in the context of the consent decree case in court and possibly other matters).

Thank you for your courtesy and attention to this question.

Respectfully,

Tim Puin
Asst. Dir., Law Dept.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Tuesday, January 2, 2024 2:31 PM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Subject: RE: OPS - public records requests

Tim-

I spoke to the Superintendent about your request. He would like to see the members of the OPS complete CJIS security training before granting them access to view those records. It can be done online and takes between 30 minutes – one hour to complete. The training is at this link: <https://www.cjisonline.com/>. When they have completed that training, let us know and furnish verification to us and then permission will be granted.

Zahid

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Thursday, January 4, 2024 11:00 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Zahid,

My colleagues are working on rolling this out internally. We are mindful of the directive that "permission will be granted" only after verification of training is sent to BCI.

My request concerned OPS but there is a different unit also made up of City employees that also conducts internal investigations of public safety personnel, like OPS, which is known as Office of Integrity Control, Compliance, and Employee Accountability (OIC). Because its role is so similar to OPS, and its members are also City employees, we will apply the same requirements to OIC employees. Thank you again for your courtesy.

On another matter:

Would the Superintendent permit non-City employee members of the federal monitoring team and U.S. DOJ to view LEADS information in the context of their work on the consent decree involving Cleveland Police, if

- (1) the members verify the same CJIS training; and
- (2) US District Judge Oliver enters a protective order in the consent decree case (*United States of America v. City of Cleveland*, N.D. Ohio No. 1:15-cv-01046-SO) preventing publication of any LEADS or other confidential information?

Currently, there is a lot of redacting that goes on before records are given to the monitoring team and DOJ, which causes delays and burdens on staff. In a previous federal court case involving the City, the Superintendent permitted dissemination of OHLEG/LEADS info for purposes of the litigation subject to a protective order. I am hoping that the same logic would apply here. The parties are not completely at odds like in the previous litigation, but are working together to implement a settlement agreement under the oversight of the monitor and the court; and there would be the added protection of requiring the CJIS training.

Thank you for addressing this additional matter at your convenience. We certainly appreciate BCI's engagement in these matters.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Puin, Timothy
To: Zahid Siddiqi
Subject: Consent decree case redactions
Date: Friday, January 5, 2024 2:38:00 PM

Zahid,

If you don't mind, please allow a brief follow up to my email 1/4/2024, which asked the following question:

Would the Superintendent permit non-City employee members of the federal monitoring team and U.S. DOJ to view LEADS information in the context of their work on the consent decree involving Cleveland Police, if

(1) the members verify the same CJIS training; and

(2) US District Judge Oliver enters a protective order in the consent decree case (*United States of America v. City of Cleveland*, N.D. Ohio No. 1:15-cv-01046-SO) preventing publication of any LEADS or other confidential information?

It was pointed out to me that the monitoring team members are not really civilians in this context. *U.S. v. Puerto Rico*, 460 F.Supp.3d 159, 161, 164 (D.P.R. 2020) ("As judicial officers of an Article III court, Monitor team members are not accountable to the Commonwealth nor Department of Justice"). Thus, it may be said that they should be allowed to view unredacted records to the same extent as the presiding Judge.

I suppose the DOJ attorneys would be more like civilians in this context. This brings to mind an email exchange we had four years ago, in which it appeared that BCI deferred to the federal district court in the management of access to confidential records through the discovery process (not to overstate or mischaracterize – please see email exchange below). Of course, FRCP 5.2, as well as local rules and standing orders, may also apply, beyond any protective order.

Hopefully these additional points help round out my question from yesterday. Thank you again very much for all of your courtesy and time spent on this issue.

Respectfully,

Tim Puin

From: Zahid Siddiqi
To: Puin, Timothy
Cc: Hough, Amy
Subject: RE: OPS - public records requests
Date: Friday, January 5, 2024 2:41:56 PM

Tim-

I apologize, but we need to hold off on this question. There has been a change in Superintendent at BCI and he is not sure about whether he will grant access. We may be in touch with additional follow up questions about the OPS and other matters. We will meet internally and get back to you.

For your other question, BCI does not administer LEADS. That is under the Ohio State Highway Patrol's purview within the Ohio Department of Public Safety. BCI can only grant consent for OHLEG access. You would need to raise questions concerning LEADS to the Department of Public Safety.

Zahid

Puin, Timothy

From: Puin, Timothy
Sent: Thursday, January 11, 2024 10:41 AM
To: klocke@dps.ohio.gov; vdowdy@dps.ohio.gov
Subject: LEADS question - follow up

Good morning.

To follow up on my 1/4/2023 email, we are asking about the chair's view of LEADS data included in records that need review for purposes of police and safety personnel oversight (by Office of Professional Standards, Office of Integrity Control, Public Safety, Monitoring Team, and related entities).

The goal is more efficient sharing of records between the first-responder divisions and their oversight bodies. Currently, the redaction process is fairly time-consuming and difficult.

LEADS data would not be used for any non-law enforcement purposes, or publicized in any way. It is just incidentally included in records. Investigators conceivably could take CJIS online training (as suggested by Supt. Morbitzer of BCI) and/or sign a confidentiality pledge acceptable to DPS.

Others from the City may have contacted you and I apologize if I missed any communications.

Thanks again very much for your valuable time and attention to this inquiry, and we look forward to hearing back from you.

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

Puin, Timothy

From: KLocke@dps.ohio.gov
Sent: Thursday, January 11, 2024 10:42 AM
To: Puin, Timothy
Subject: Automatic reply: [EXTERNAL]LEADS question - follow up

I am currently out of the office with limited access to email. Please use the following contacts in my absence:

LEADS Administration – Victoria Dowdy (vdowdy@dps.ohio.gov)

LEADS Operations – Richard Bussey (rabussey@dps.ohio.gov)

Computer Operations – Mauro Pereira (mpereira@dps.ohio.gov)

Network Operations – Jeremy Ebert (jebert@dps.ohio.gov)

LEADS Programming – Kate Hatfield (Kharfield@dps.ohio.gov)

LEADS Security – Tom Brisco (Tbrisco@dps.ohio.gov) or LEADSSecurity@dps.ohio.gov

If you require immediate assistance, please contact LEADS Control at 614-466-3055.

Puin, Timothy

From: Puin, Timothy
Sent: Thursday, January 11, 2024 10:44 AM
To: rabussey@dps.ohio.gov; tbrisco@dps.ohio.gov
Subject: FW: LEADS question - follow up

Sirs,

Based on Mr. Locke's out of office message, the email below is being forward to you.

Respectfully,

Tim Puin

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Puin, Timothy
Sent: Thursday, January 11, 2024 10:41 AM
To: klocke@dps.ohio.gov; vdowdy@dps.ohio.gov
Subject: LEADS question - follow up

Good morning.

To follow up on my 1/4/2023 email, we are asking about the chair's view of LEADS data included in records that need review for purposes of police and safety personnel oversight (by Office of Professional Standards, Office of Integrity Control, Public Safety, Monitoring Team, and related entities).

The goal is more efficient sharing of records between the first-responder divisions and their oversight bodies. Currently, the redaction process is fairly time-consuming and difficult.

LEADS data would not be used for any non-law enforcement purposes, or publicized in any way. It is just incidentally included in records. Investigators conceivably could take CJIS online training (as suggested by Supt. Morbitzer of BCI) and/or sign a confidentiality pledge acceptable to DPS.

Others from the City may have contacted you and I apologize if I missed any communications.

Thanks again very much for your valuable time and attention to this inquiry, and we look forward to hearing back from you.

Timothy J. Puin

Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

Puin, Timothy

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Friday, January 12, 2024 11:07 AM
To: Puin, Timothy
Cc: Hough, Amy
Subject: RE: OPS - public records requests

Tim-

After an internal meeting and review of the OHLEG Rules and Regulations (Regulations), the Superintendent does not believe he can grant consent to the City for the Office of Professional Standards (OPS) to access OHLEG records and materials. When examining the Regulations, a few sections stand out to us in our analysis.

The Regulations define a criminal justice agency as "The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included." Page 4. The definitions also define law enforcement agency as "A police department, the office of a sheriff, the state highway patrol, a county prosecuting attorney, or a federal, state, or local governmental body that enforces criminal laws and has employees who have a statutory power of arrest." Page 5. Absent from these definitions is a civilian review board such as the OPS. In addition, the OPS lacks the statutory authority to arrest and does not allocate a substantial part of its budget to the administration of criminal justice.

When examining other provisions, we noted the definition of secondary dissemination, defined as "The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement." Page 8. We are not convinced that OPS is an authorized recipient agency due to it being neither a criminal justice agency nor a law enforcement agency. This is supported by Regulation 4.0, which reads:

CJI shall only be used and disseminated consistent with the authorized purpose for which it was accessed. Dissemination of CJI to another agency is authorized if (a) the other agency is an authorized recipient of such information, or (b) the other agency is performing personnel and appointment functions with codified authority to obtain CJI for criminal justice employment applicants.

Regulation 4.0, Page 24. Based on our understanding of OPS' mission, we do not feel that OPS fits that definition.

If you can share more information about OPS and its mission, we can discuss further. But as it currently stands, we don't feel the Regulations authorize the dissemination of OHLEG materials to the OPS.

Feel free to reach out should you have questions or concerns.

Respectfully,

Zahid



Zahid H. Siddiqi
Chief Counsel – BCI
Office of Ohio Attorney General Dave Yost
1560 S.R. 56 S.W.
London, OH 43140
Office: 740-845-2185

Mobile: 614-264-6650
Zahid.Siddiqi@OhioAGO.gov

Confidentiality Notice: This message is intended for use only by the individual or entity to whom or which it is addressed and may contain information that is privileged, confidential and/or otherwise exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by telephone.

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Friday, January 5, 2024 2:43 PM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Understood, thank you sir!

We will follow up but your time is greatly appreciated.

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

From: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Sent: Friday, January 5, 2024 2:42 PM
To: Puin, Timothy <tpuin@clevelandohio.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

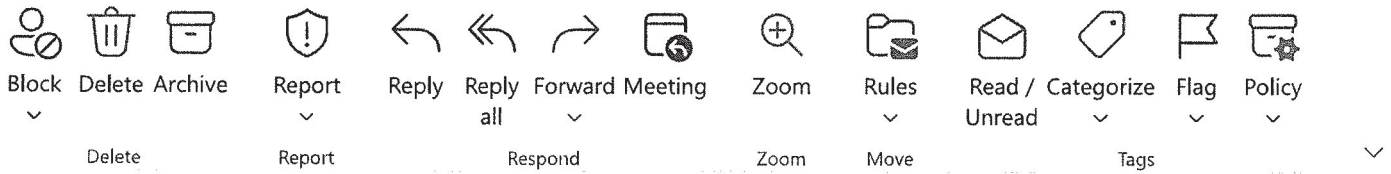
Tim-

I apologize, but we need to hold off on this question. There has been a change in Superintendent at BCI and he is not sure about whether he will grant access. We may be in touch with additional follow up questions about the OPS and other matters. We will meet internally and get back to you.

For your other question, BCI does not administer LEADS. That is under the Ohio State Highway Patrol's purview within the Ohio Department of Public Safety. BCI can only grant consent for OHLEG access. You would need to raise questions concerning LEADS to the Department of Public Safety.

Zahid

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Thursday, January 4, 2024 11:00 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>



RE: OPS - public records requests

This message is encrypted. What's encryption?

You replied on Fri 1/12/2024 11:29 AM

ZS Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
To: Puin, Timothy
Cc: Hough, Amy

...
Fri 1/12/2024 11:28 AM

OHLEG_Rules_Regulations 0222...
405 KB

I have also attached the rules for your own analysis. Feel free to reach out with questions.

Zahid

From: Puin, Timothy <tpuin@clevelandohio.gov>
Sent: Friday, January 12, 2024 11:19 AM
To: Zahid Siddiqi <Zahid.Siddiqi@OhioAGO.gov>
Cc: Hough, Amy <AHough@clevelandohio.gov>
Subject: RE: OPS - public records requests

Zahid,

Thank you to you, the Superintendent, and all concerned, for the time and attention to this inquiry. I will forward your response to the officials involved here in Cleveland and follow up with you if they wish to discuss further.

Respectfully,

Tim

Timothy J. Puin
Asst. Director, Dept. of Law
City of Cleveland
601 Lakeside Ave. E., Room 106
Cleveland, Ohio 44114-1077
216-664-2807

NOTICE: This email is intended only for the use of the party to which it is addressed and may contain information that is privileged, confidential, or protected by law. If you are not the intended recipient, you are hereby notified that any dissemination, copying or distribution of this email or its contents is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.



Rules and Regulations

Effective February 22, 2017

Contents

Contact Information	3
Terms and Definitions	3
Acronym List	8
Introduction	9
Access	10
1.0 OHLEG Agency/User Agreements	10
1.1 Access Restrictions	10
1.2 Access Control Criteria	11
1.3 System Use Notification	11
1.4 Personnel Security	12
1.5 OHLEG Access Procedure	13
1.6 New Agency OHLEG Application	14
1.7 Out-of-State Agency OHLEG Application	14
1.8 Security Awareness Training	16
1.9 All Personnel	16
1.10 OHLEG Practice and Test Inquiries	17
1.11 Facial Recognition	17
Management	19
2.0 Participating Agency Chief Executive Responsibility	19
2.1 User Account Management	19
2.2 OHLEG Agency Approver	20
2.3 OHLEG Agency Coordinator	20
2.4 Personnel Termination	21
2.5 Personnel Action	21
2.6 OHLEG Sanctions	21
2.7 Agency Sanctions	22
Quality Assurance	22
3.0 Monitoring, Analysis, and Reporting	22
3.1 Special Security Inquiries and Audits	23

3.2	Audit Log Retention	23
3.3	Agency Audit Requests.....	23
3.4	Reporting	24
	Data Security	24
4.0	Criminal Justice Information (CJI)	24
4.1	Criminal History Record Information (CHRI)	25
4.2	Personally Identifiable Information (PII)	25
4.3	Dissemination.....	26
4.4	Dissemination of CJI Related to Discovery Motion.....	26
4.5	CHRI Storage	26
4.6	Passwords	27
4.7	Physical Protection.....	27
4.8	Controlled Area	28
4.9	Personally Owned Information Systems.....	28
4.10	Publicly Accessible Computers.....	28
4.11	Mobile Technologies	28
4.12	Cellular Risk Mitigations	29
4.13	Media Protection	29
4.14	Electronic Media Sanitization and Disposal.....	30
4.15	Disposal of Physical Media.....	30
	Technical Compliance.....	30
5.0	Device and Resource Protection Guidelines	30
5.1	Data Security Threat Incident Response.....	32
	Appendix A: OHLEG Practice and Test Inquiries	33
	Appendix B: Model OHLEG Policy	34
	Appendix C: Referenced Ohio Revised Code.....	38

Contact Information

OHLEG Support:

Main Phone: (866) 406-4534

Email: OHLegSupport@OhioAttorneyGeneral.gov

BCI Radio Room:

Main Phone: (740) 845-2224

OHLEG Quality Assurance:

Email: OHLEGQualityAssurance@OhioAttorneyGeneral.gov

Terms and Definitions

Access to Criminal Justice Information - The physical or logical (electronic) ability, right or privilege to view, modify, or make use of Criminal Justice Information (CJI).

Administration of Criminal Justice - The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes “crime prevention programs” to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g., record checks of individuals who participate in Neighborhood Watch or “safe house” programs) and the result of such checks will not be disseminated outside the law enforcement agency.

AGO IT - The information technology section of the Ohio Attorney General’s Office.

Authorized Use - The act of using OHLEG in a manner that is consistent with OHLEG security policies, Ohio Revised Code, and with the criminal justice purposes for which the user was granted OHLEG access.

Biographic Data - Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data - When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case/Incident History - All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regard to CJI, it is the information about the history of criminal incidents.

Criminal History Record Information (CHRI) - A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information, or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) - The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Information (CJI) - Criminal Justice Information is the abstract term used to refer to all of the OHLEG-provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data.

Criminal Justice Purpose - The motivating reason behind a user action, derived from the user's work related duties or needs in furtherance of the administration of criminal justice.

Department of Justice (DOJ) - The department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just

punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Dissemination - The transmission/distribution of CJI to another person or agency.

Encrypted (data) - Computer data that is converted into an incomprehensible form through the use of a key. Only a holder of a matching key can restore the data to its original form.

Facial Recognition (FR) - An OHLEG attribute that allows unidentified photos from a police investigation to be searched by facial feature comparison against a database of known person's photos.

Information System - A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Law Enforcement Activity (as used in Section 1.11 Facial Recognition) - An activity, carried out by duly authorized law enforcement personnel pursuant to their official duties, that is consistent with law and is grounded in a reasonable belief based on a totality of circumstances that the use of facial recognition may result in an investigative lead with respect to a specific criminal matter; reduce an imminent threat to health or safety; or assist in the identification of someone who is not able to identify him or herself.

Law Enforcement Agency - A police department, the office of a sheriff, the state highway patrol, a county prosecuting attorney, or a federal, state, or local governmental body that enforces criminal laws and has employees who have a statutory power of arrest.

Logical Access - In computer security, being able to interact with data through access control procedures such as identification, authentication and authorization.

Misuse - Any utilization of OHLEG that is not directly related to the administration of criminal justice, or that is inconsistent with OHLEG security policies, Ohio Revised Code, Ohio Administrative Code, or the criminal justice purposes for which the user was granted OHLEG access. This includes, but is not limited to, uses motivated by the personal interest of the user or for the user's commercial benefit, as determined by the Director of OHLEG.

OHLEG Agency Approver (Approver) - An OHLEG user designated by the agency CEO to approve OHLEG Access Applications.

OHLEG Agency Coordinator (OAC) - An OHLEG user who will serve as the point of contact at each OHLEG Participating Agency with specific duties and responsibilities for administering OHLEG security policies in support of the agency CEO.

OHLEG Agency Identifier (OAI) - An alphanumeric agency identifier which could be either a CJIS-issued ORI or an OHLEG-issued equivalent for agencies unable to obtain an ORI.

OHLEG Agency/User Agreement - A terms-of-service acknowledgment that must be signed prior to obtaining agency or individual user OHLEG access. This acknowledgment must be signed on behalf of the agency and also by each individual user.

OHLEG Director - Senior staff member of BCI administration responsible for oversight and administration of all OHLEG-related functions in support of the Superintendent of BCI.

OHLEG Executive Management - The Superintendent of the Ohio Bureau of Criminal Investigation, the Assistant Superintendent of BCI, and the OHLEG Director.

OHLEG Participating Agency (Agency) - A criminal justice agency (CJA) that has been granted access to OHLEG.

OHLEG Security Policies - The term used to encompass all forms of guidance or directives used by OHLEG to control and direct OHLEG agency and user access, usage, behavior and conduct. This term includes but is not limited to: OHLEG Rules and Regulations, OHLEG site notifications and acknowledgements, and OHLEG directives, messages, and security training videos.

OHLEG User - An individual authorized to access OHLEG, who has been appropriately vetted through a national fingerprint-based record check and has been granted access to CJI data.

Personal Use - Use of OHLEG, outside of official business for the agency.

Personally Identifiable Information (PII) - Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name and date of birth, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Probationary Access (Probation) - A sanction which requires a period of supervised OHLEG usage before being restored to full OHLEG access.

Property Data - Information about vehicles and property associated with a crime.

Task Force - A group initiative involving the structured, organized, collaborative effort of multiple law enforcement agencies that targets a particular criminal activity, often in a particular geographical area.

Secondary Dissemination - The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Incident - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. These include but are not limited to: attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Validation - An action performed by either a participating agency or OHLEG auditors or administration to verify that OHLEG user authorizations, access, training and other security policy requirements are accurate, appropriate and up to date.

Acronym List

AGO	Attorney General's Office
BCI	Ohio Bureau of Criminal Investigation
CEO	Chief Executive Officer
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
LEADS	Law Enforcement Automated Data System
OAC	OHLEG Agency Coordinator
OAI	OHLEG Agency Identifier
OHLEG	Ohio Law Enforcement Gateway
ORC	Ohio Revised Code
ORI	Originating Agency Identifier
PII	Personally Identifiable Information
QAS	Quality Assurance Specialists

Introduction

The Ohio Attorney General created the Ohio Law Enforcement Gateway (OHLEG) to allow practitioners to have timely and secure access to criminal justice data. The OHLEG Rules and Regulations were created for criminal justice agencies using OHLEG to ensure that the sources, transmission, storage, and generation of Criminal Justice Information (CJI) are protected.

The OHLEG Rules and Regulations apply to every OHLEG user as well as non-user members of Criminal Justice Agencies (CJA) who handle Criminal Justice Information obtained through OHLEG in the course of their duties.

The Rules and Regulations are designed to allow sufficient flexibility for participating agencies to structure their security programs according to their needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this document.

The OHLEG staff developed the first version of the OHLEG Rules in April 2005. The rules were expanded in June 2014 to address the privacy concerns of Ohio citizens related to newly developed OHLEG software applications. This updated version of OHLEG Rules refines the expanded rules and incorporates the OHLEG Data Security Use Policy into the Rules and Regulations document.

All OHLEG users are required to read and abide by the OHLEG Rules and Regulations. OHLEG quality assurance provides assistance with agency audits and investigations and works to ensure compliance with rules and regulations. OHLEG support works tirelessly to keep users' account access functioning and accessible. OHLEG administration's goal is to keep this invaluable tool available for use by criminal justice agencies working to protect the citizens of Ohio while respecting the privacy rights of those same citizens. Assisting in this effort OHLEG would like to acknowledge the contribution and assistance of the OHLEG Advisory and Steering Committees in the development and production of this rules and regulations document. Their valued counsel contributes significantly toward the achievement of this goal.

Access

1.0 OHLEG Agency/User Agreements

Any CJA receiving access to OHLEG must sign the OHLEG Agency/User Agreement. The agency CEO will sign an agreement on behalf of the agency. By signing this agreement, the agency acknowledges that it is responsible for enforcing and adhering to all OHLEG Security Policies, as well as accepting responsibility for all users gaining access through that agency.

Additionally, each individual user must also sign an OHLEG Agency/User agreement. The individual user agreements will be kept on file at the agency, where they will be subject to inspection by OHLEG Quality Assurance. By signing this agreement, all users acknowledge they are responsible for reading and understanding all OHLEG Security Policies and will be held accountable for violating them. All users also acknowledge that access to OHLEG is limited to use for criminal justice purposes only. OHLEG access is NOT to be used for personal use.

The OHLEG Agency/User Agreement is available on the OHLEG website.

The law enforcement data maintained by BCI on the OHLEG site is provided at and subject to the discretion of BCI. BCI's grant of access to OHLEG confers no process or other rights in maintaining such access.

1.1 Access Restrictions

Criminal justice professionals who work for a law enforcement agency (e.g., police officers and sheriff's deputies) require a greater degree of OHLEG access than those who work for non-law enforcement agencies (e.g., court employees). For this reason OHLEG law enforcement users will be given access to a wider range of OHLEG attributes than will non-law enforcement users.

The CEO of each agency bears the primary responsibility for determining and enforcing access restrictions. OHLEG users are permitted only to access OHLEG attributes that are directly related to their job responsibilities. Access to individual attributes shall be based on the agency to which the user is assigned at the time of use. OHLEG users who participate through multiple agencies shall only log on to OHLEG using the OAI number for the

agency for which they are working at the time of access. The attributes are to be determined by the CEO or designee at the time of the user's request for access and should be reviewed when job assignments or responsibilities change. Task Force members wishing to obtain a separate OHLEG account as part of their Task Force duties should contact the BCI/OHLEG Support Center.

The nexus between an account holder's job assignment and OHLEG access is subject to review and validation during OHLEG Quality Assurance visits. Furthermore, users shall not attempt to access any data, documents, email correspondence, and/or programs contained on BCI/OHLEG information resources for which they do not have authorization.

1.2 Access Control Criteria

Agencies should consider the following when establishing rules that control access to CJI:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
4. Time-of-day and day-of-week/month restrictions.

1.3 System Use Notification

OHLEG will display an approved system use notification message, before granting access, informing potential users of various usage and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. Unauthorized use of the system is prohibited and a violation of criminal law.
3. System usage is subject to monitoring, recording, and auditing.

4. Use of the system indicates consent to monitoring and recording. The system includes all data, software, media, and hardware.
5. The law enforcement data maintained by BCI on the OHLEG site is provided at and subject to the discretion of BCI. BCI's grant of access to OHLEG confers upon the user no process or other rights in maintaining such access.

The system use notification message and any communications must be acknowledged before the user can gain access to the system.

1.4 Personnel Security

Having proper security measures against the insider threat is a critical component of the OHLEG security policies. This section's security terms and requirements apply to all personnel who have access to OHLEG including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI. Access to OHLEG is a privilege and not a right.

The minimum screening requirements for individuals requiring access to CJI are as follows:

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to OHLEG or CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to OHLEG.
2. The agency CEO shall specify the agency process for requesting OHLEG access.
3. If a felony conviction of any kind exists, the agency CEO shall deny access to OHLEG. However, the CEO may ask for a review by the OHLEG Director in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

4. If the person has a non-felony conviction or any arrest history without conviction, access to CJI shall not be granted until the agency CEO reviews the matter to determine if access is appropriate.
5. If the person has an arrest history that includes any theft, domestic violence, menacing, or stalking offense; telecommunications harassment; or any misuse of OHLEG, LEADS, or misuse of any law enforcement restricted database or information, the CEO shall deny access. The CEO may ask for a review by the OHLEG Director as indicated in #3 above.
6. If the person appears to be a fugitive the person will be denied access to OHLEG.
7. If the person already has access to CJI and is subsequently arrested and/or convicted of a crime, access to OHLEG shall be terminated. If the crime is a non-felony, OHLEG access may be reinstated following a review by the agency CEO consistent with #4 and #5 above.
8. If the agency CEO, OAC, or OHLEG Director determines that access to OHLEG by an applicant/user would not be in the public interest, access shall be denied/removed. If access is denied/removed under this section, the agency shall notify the BCI/OHLEG Support Center in writing.
9. BCI/OHLEG's determination as to an OHLEG user's status is independent of, and unrelated to, his/her employment situation with their agency. BCI will not make any determination about an OHLEG user's job status, a matter over which BCI exercises no authority or discretion.

1.5 OHLEG Access Procedure

No OHLEG user shall attempt to gain access to OHLEG or any OHLEG attribute beyond the specific access limits established and authorized by his or her employing agency.

1. Requests for OHLEG access will be made via the OHLEG Online Account Application attribute, which is available on the homepage of any current OHLEG user.
2. On each new user application, the Approver is required to certify that the basic training security video for a new OHLEG user has been viewed by

the applicant. The Approver must also certify that the OHLEG Agency/User Agreement has been signed by the user.

3. The new applicant must then physically enter his or her personal information in the appropriate sections on the online application.
4. The Approver will select from a checklist which available OHLEG attributes are approved for each applicant.
5. The Approver shall submit applications electronically to OHLEG administration for further processing and activation.
6. The Facial Recognition attribute will require specific authorization by the CEO and justification for each user indicating the investigative or other area of responsibility requiring such access.
7. Non-law enforcement agencies generally will not have access to the Facial Recognition attribute. Any non-law enforcement agency believing it has an exceptional need for access to the Facial Recognition attribute may apply to the Superintendent of BCI for Facial Recognition access.

1.6 New Agency OHLEG Application

All agencies new to OHLEG must complete a New Agency Application form. Please contact the BCI/OHLEG Support Center to request this form.

1.7 Out-of-State Agency OHLEG Application

OHLEG allows out-of-state law enforcement agencies to have OHLEG access based on specific need. This need may be indicated by an Ohio border jurisdiction or an Ohio related investigation. Such access serves the mutual interest of law enforcement agencies outside of Ohio and Ohio criminal justice. Out-of-state law enforcement agencies may apply for OHLEG access as an OHLEG Participating Agency.

Procedure:

1. The out-of-state law enforcement agency must apply for agency status by filling out the OHLEG Out-of-State Agency Application, which can be found on OHLEG or obtained from the BCI/OHLEG Support Center.
2. The application must state the specific criminal justice purpose OHLEG access will meet for the applying agency and how OHLEG access will be used if granted.
3. If granted, only OHLEG attributes related to the specific needs of the agency will be authorized.
4. OHLEG access granted to any out-of-state law enforcement agency will be for a limited specific time period not to exceed one year. Out-of-state access is renewable through the application process on a yearly basis.
5. The applying agency must acknowledge its understanding that misuse of OHLEG constitutes a criminal violation of Ohio law and that such cases will be turned over to an Ohio county prosecuting attorney for prosecution under the applicable Ohio statute.
6. Out-of-state law enforcement agencies will be required to adhere to OHLEG security policies including CEO supervision and audit compliance.
7. Out-of-state law enforcement agencies as a general rule will not have access to the Facial Recognition attribute. Any out-of-state law enforcement agency believing it has an exceptional need for access to the Facial Recognition attribute may apply to the Superintendent of BCI for Facial Recognition access.
8. Out-of-state, non-law enforcement criminal justice agencies will not be granted OHLEG access without the express written authorization of the Superintendent of BCI.

1.8 Security Awareness Training

An OHLEG Security Training Video will be made available online. Viewing of the OHLEG Security Awareness Training video shall be required before OHLEG access and initial assignment credentials are issued. Security awareness training will be required every two years thereafter for all personnel with access to OHLEG. This biennial training can be accomplished by watching the current OHLEG Security Training video or by completing agency security awareness training that meets the requirements in Section 1.9. The agency shall document user training and provide such documentation upon request. Note that the AGO/BCI/OHLEG may require additional security awareness training and will provide training if necessary.

1.9 All Personnel

At a minimum, the following topics shall be addressed as security awareness training for all authorized personnel with access to OHLEG:

1. Rules that describe responsibilities and expected behavior with regard to OHLEG system usage.
2. Implications of noncompliance.
3. Incident response (points of contact; individual actions).
4. Media protection.
5. Password usage and management – including creation, frequency of changes, and protection.
6. Protection from viruses, worms, Trojan horses, and other malicious code.
7. Unknown e-mail/attachments.
8. Web usage – allowed versus prohibited; monitoring of user activity.
9. Spam.
10. Social engineering.
11. Physical Security – increases in risks to systems and data.
12. Handheld device security issues – address both physical and wireless security issues.

13. Laptop security – address both physical and information security issues.
14. Personally owned equipment and software – state whether allowed or not (e.g., copyrights).
15. Access control issues – address least privilege and separation of duties.
16. Individual accountability – explain what this means in the agency.
17. Use of acknowledgement statements – passwords, access to systems and data, and personal use.
18. Desktop security – discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
19. Protecting information subject to confidentiality concerns – in systems, archived, on backup media, and until destroyed.
20. Dissemination and destruction.

1.10 OHLEG Practice and Test Inquiries

In order for OHLEG users to familiarize themselves with the OHLEG Search Engine (SE) or to test system functionality, practice/test inquiries have been provided and posted onto OHLEG and are attached in Appendix A of this document. **OHLEG USERS ARE NOT ALLOWED TO RUN SEARCHES ON THEMSELVES OR FAMILY MEMBERS**—such searches will trigger an audit by OHLEG Quality Assurance.

1.11 Facial Recognition

Facial recognition technology is an investigative tool. Law enforcement should use it to generate an investigative lead in an active criminal matter in order to solve or prevent crime, to reduce an imminent threat to health or safety, or to identify someone who is not able to identify himself or herself. Law enforcement may not employ this technology to conduct dragnet screening of individuals, nor should it use it to facilitate mass surveillance of places, groups, or activities unless doing so furthers an official law enforcement activity. For example, it would not be appropriate for law enforcement to use facial recognition technology to conduct surveillance of persons or groups based solely on their religious, political, or other

constitutionally protected activities or affiliations unless doing so furthers an official law enforcement activity.

The use of the Facial Recognition attribute as an investigative tool will fall under the same rules as those applied to OHLEG CJI with the addition of the following:

1. All Ohio drivers' licenses, ID photos, and all other photos will remain in the custody and control of the originating agency or OHLEG but will not be otherwise transferred to any other entity.
2. Images received in a request or submission will not be stored as enrolled images within the Facial Recognition system. A thumbnail photo will be archived for audit purposes, but the photo will not be enrolled in the database and will not be searchable.
3. Images enrolled in the Facial Recognition system will not be released to anyone other than law enforcement personnel and only in conjunction with an authorized criminal investigation.
4. Facial Recognition technology may only be used for an official law enforcement activity. For the purposes of this section, an "official law enforcement activity" shall mean an activity, carried out by duly authorized law enforcement personnel pursuant to their official duties, that is consistent with law and is grounded in a reasonable belief based on a totality of circumstances that the use of facial recognition may:
 - a. Result in an investigative lead with respect to a specific criminal matter;
 - b. Reduce an imminent threat to health or safety;
 - c. Assist in the identification of someone who is not able to identify him or herself.
5. Agencies must keep a log with an entry, showing the date, name, case number, and the type of criminal investigation being conducted, for every use of the Facial Recognition attribute.

6. All Facial Recognition requests and any results of the inquiry will be maintained by OHLEG in accordance with appropriate current OHLEG document maintenance and destruction policies.
7. An agency supervisor must approve any dissemination of Facial Recognition images or search results beyond the originating agency.
8. Disseminations to the press will occur only with OHLEG management and requesting agency authorization.

Management

2.0 Participating Agency (Agency) Chief Executive Responsibility

All OHLEG Participating Agencies are responsible for establishing and administering an OHLEG security program throughout the agency's user community. The Chief Executive Officer (CEO) of each agency is responsible for that agency's adherence to OHLEG security policies. That responsibility includes accountability for individual OHLEG account holders within the CEO's agency. The agency CEO shall appoint an OHLEG Agency Approver and Coordinator. The agency CEO may choose to fill either or both roles him or herself. The CEO, OAC, and Approver will be given access to the OHLEG Roster attribute through which they can manage user account access. The agency may impose more stringent protection measures than those outlined in the OHLEG security policies. Such measures shall be documented and kept current.

2.1 User Account Management

The agency shall manage OHLEG accounts, including applications, training, modifying and reviewing accounts, and validating rosters.

The agency shall grant continued access to the information system based on:

1. Valid need-to-know that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

2.2 OHLEG Agency Approver (Approver)

The Approver is an individual located within the agency responsible for approving OHLEG Access Applications. They are unable to approve Facial Recognition requests, which with limited exceptions must be approved by the agency CEO.

2.3 OHLEG Agency Coordinator (OAC)

The OAC is an individual located within the agency who serves as the main contact person for OHLEG and is responsible for the administration of the OHLEG network for the agency. The agency CEO—through the OAC—shall:

1. Validate the agency OHLEG roster every 90 days. This validation process requires the OAC to confirm that all users listed on the roster are current employees and authorized OHLEG users.
2. Set, maintain, and enforce standards for the selection, supervision, and separation of personnel who have access to OHLEG.
3. Oversee by all appropriate means the adherence by the agency and its users to all OHLEG security policies.
4. Document technical compliance with OHLEG security policies with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the agency's user community.
5. Establish a data security threat incident response and reporting procedure to discover, investigate, document, and report to the agency CEO and OHLEG, incidents that endanger the security or integrity of CJI.
6. Ensure that personnel security screening procedures are being followed as stated in these regulations.
7. Ensure that the approved and appropriate security measures are in place and working as expected.
8. Report data security threat incidents as outlined in Section 5.1.

2.4 Personnel Termination

The agency, upon termination of an individual's employment, shall immediately remove the individual's access to OHLEG through OHLEG Roster or by notifying the BCI/OHLEG Support Center. If the termination is related to OHLEG misuse, the agency CEO or OAC shall notify the BCI/OHLEG Support Center. If the termination is related to other misconduct, the CEO or OAC should consider requesting the user's audit log from OHLEG so the agency can determine whether OHLEG misuse may also have occurred.

2.5 Personnel Action

The agency shall review OHLEG access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing accounts and changing system access authorizations. The agency is also responsible to notify the BCI/OHLEG Support Center and submit new designations whenever there is a personnel change affecting the OHLEG roles of agency CEO, OAC, and/or Approver.

If an OHLEG user is removed from full active duty as a result of a personnel action, including but not limited to, suspension, administrative leave, or disciplinary action, the OAC will initiate an Administrative Review to determine if the user should have access during said removal.

2.6 OHLEG Sanctions

The law enforcement data maintained by BCI on the OHLEG site is provided at, and subject to, the discretion of BCI. BCI's grant of access to OHLEG does not confer upon the agency or its users any process or other rights in maintaining such access. Termination of rights for BCI/OHLEG information resources may also be applied to other AGO information resources services and/or products.

OHLEG sanctions for violations of OHLEG security policies may include any of the following disciplinary actions:

1. Criminal prosecution.
2. Permanent termination of user or agency access.

3. Suspension of user or agency access.
4. Probationary user or agency access.
5. Restricted user or agency access.
6. Mandatory user or agency re-training.

2.7 Agency Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established OHLEG security policies. See Section 3.4 for additional rules governing OHLEG misuse.

Agency sanctions for user misuse **may** also include the following:

1. Termination of employment.
2. Unpaid suspension of employment.
3. Reprimand.
4. Training or re-training.
5. Performance improvement plan.

Quality Assurance

3.0 Monitoring, Analysis, and Reporting

Electronic files created, sent, and received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of the AGO are the property of the AGO and use of such information is neither personal nor private.

OHLEG Access is to be used for criminal justice purposes only. Personal use is strictly forbidden.

OHLEG shall employ Quality Assurance Specialists (QAS) to perform audits to ensure compliance with OHLEG security policies including those applying to both agencies and OHLEG users. OHLEG QAS shall visit agencies to perform audits to ensure this compliance. Random audits shall also be conducted as a matter of course and shall not require a complaint, alleged security violation, or other justification.

OHLEG QAS shall routinely review and analyze agency audit records for suspicious activity or indications of misuse. OHLEG QAS will assist in the investigation of suspected violations and report findings to the appropriate officials.

3.1 Special Security Inquiries and Audits

All agencies having access to OHLEG shall permit an OHLEG Quality Assurance inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the OHLEG Director. All results of the inquiry and audit shall be reported to the agency CEO and OHLEG Director with appropriate recommendations.

3.2 Audit Log Retention

All log records of OHLEG usage kept by the agency, including but not limited to Facial Recognition inquiries and CHRI dissemination logs, are subject to audit at any time. These logs shall be maintained for a minimum period of eight years or a period equal to the agency's internal record retention policy – whichever is greater.

3.3 Agency Audit Requests

An agency may request an audit of an agency employee's OHLEG usage. This audit may be requested as part of an investigation conducted by the agency or as a routine part of agency initiated monitoring. The audit must be requested by either the agency CEO or OAC.

A law enforcement agency, with proper jurisdiction, may find it necessary to conduct a criminal investigation of a user employed by an OHLEG Participating Agency. In such circumstances, the investigating agency may request an OHLEG audit of the subject under investigation. A request for an OHLEG audit of another agency's user must come from the investigating

agency CEO on department letterhead and indicate it is requested as part of a criminal investigation.

OHLEG audit requests may be requested via email at OHLEGQualityAssurance@OhioAttorneyGeneral.gov.

Upon completion of any investigation of OHLEG misuse, the law enforcement agency will forward a copy of the full investigative report to OHLEG for administrative review.

3.4 Reporting

All users shall address any questions regarding policy, responsibilities, and duties to the BCI/OHLEG Support Center or OHLEG Quality Assurance. If an agency CEO, OAC, or any user either suspects misuse or knows of a violation of OHLEG security policies, it is their duty to take immediate action to contact OHLEG. The agency CEO or OAC may suspend an account at any time if they suspect misuse. If misuse is found, the account should be suspended to prevent further misuse. Additionally, all users shall immediately report to the BCI/OHLEG Support Center any known or suspected security incidents or improper use of OHLEG, whether or not such event resulted in an unauthorized disclosure.

Data Security

4.0 Criminal Justice Information (CJI)

It is the intention of OHLEG to ensure the protection of Criminal Justice Information until such time as the information is either released to the public via authorized dissemination (e.g., within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

CJI shall only be used and disseminated consistent with the authorized purpose for which it was accessed. Dissemination of CJI to another agency is authorized if (a) the other agency is an authorized recipient of such information, or (b) the other agency is performing personnel and appointment functions with codified authority to obtain CJI for criminal justice employment applicants.

The following rules would apply when dealing with OHLEG data:

1. Make printouts unreadable prior to disposal.
2. Before exchanging OHLEG data, agencies must have formal agreements in place that specify security controls.
3. Do not email, transport, or store OHLEG information on electronic media unless it is encrypted.

4.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI) is a subset of CJI. Due to its sensitive nature, additional controls are required for the access, use and dissemination of CHRI.

The dissemination of CHRI to any person outside of the participating agency shall be logged by the participating agency. The following dissemination information shall be logged:

1. Date.
2. Recipient agency and OAI.
3. Record type.
4. Method or means (fax, hard-copy distribution, e-mail, etc.).
5. Person who disseminated.
6. Person who received.

4.2 Personally Identifiable Information (PII)

OHLEG-provided data maintained by an agency, including but not limited to, education, financial transactions, and criminal or employment history may include PII. A criminal history record, for example, inherently contains PII.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

4.3 Dissemination

CJI obtained through OHLEG may not be used or disseminated beyond the implied or expressed consent of the Superintendent of the Bureau of Criminal Investigation. Use and dissemination is deemed to be within the scope of the Superintendent's consent when it is provided to a criminal justice agency or a defendant's counsel, in accordance with dissemination restrictions specified herein at Section 4.4.

4.4 Dissemination of CJI Related to Discovery Motion

CJI obtained through OHLEG routinely becomes a part of investigative case files provided to the county or federal prosecutor. When a prosecutor determines that OHLEG output should be given to defense counsel in response to a demand for discovery under a Rule of Criminal Procedure, a prosecutor may turn the OHLEG output over to defendant's counsel. In such cases, all CJI obtained via OHLEG shall be marked "counsel only." In addition, defense counsel should be advised in writing that "The criminal justice information obtained via the Ohio Law Enforcement Gateway is protected pursuant to ORC 2913.04(D). Dissemination of this information beyond defense counsel is considered a misuse of information obtained via the Ohio Law Enforcement Gateway and will be prosecuted accordingly. Dissemination beyond defense counsel or defense counsel's agents or employees may constitute a violation of Ohio Criminal Rule 16(C) and subject counsel to further disciplinary action." The limitations and provisions of this section do not apply to laboratory reports that are disseminated for criminal discovery purposes through OHLEG.

4.5 CHRI Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files.

4.6 Passwords

All users acknowledge that it is their responsibility to protect the information contained in OHLEG to the best of their ability and that they are solely responsible for all activities performed under their account. Therefore, users should use unique accounts and passwords for all systems and never share accounts or passwords with any other person or use any other person's accounts and passwords to access any BCI/OHLEG information resource. Users should use screen locks with password protection on all devices used to access BCI/OHLEG information resources. Users shall not share their account(s), passwords, Personal Identification (PIN), Security Tokens (e.g., Smartcard), or similar information or devices used for identification and authorization purposes. Additionally, strong passwords should be used on all devices used to access BCI/OHLEG information resources.

4.7 Physical Protection

The agency must ensure that OHLEG CJI and information system hardware, software, and media are physically protected in a manner and location that does not allow unauthorized persons to view or have access to CJI. Users shall operate systems and technology only in a secure environment and when not in use, they should be secured to ensure that unauthorized access does not occur. This protection should include the following:

1. A secure facility with physical and personnel security controls which allow access only to approved personnel.
2. The location of physical display media such as monitors so that they cannot be viewed by unauthorized personnel.
3. Visitor control that ensures no visitors are left unescorted in areas with access to CJI or information hardware, software, or media.
4. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas shall be subject to state and national fingerprint-based record checks unless these individuals are escorted by authorized personnel at all times.

4.8 Controlled Area

If an agency cannot meet all the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a “controlled area” for the purpose of day-to-day CJI access or storage.

The agency shall at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
 2. Lock the area, room, or storage container when unattended.
 3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
- The physical protection standards listed in 4.7 and 4.8 apply to an agency’s physical facility. Please refer to sections 4.11 and 4.12 for rules governing mobile technologies.

4.9 Personally Owned Information Systems

A personally owned computer or other digital device shall not be authorized to access, process, store, or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned computer usage. This control does not apply to the use of personally owned computers to access the agency’s information systems and information that is intended for public access.

4.10 Publicly Accessible Computers

Using publicly accessible computers to access OHLEG is prohibited. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, and public kiosk computers.

4.11 Mobile Technologies

Cellular telephones, smartphones (e.g., Blackberry, iPhones, etc.), tablets, iPads, laptops, and “air cards” are examples of cellular handheld devices or devices that employ cellular technology. Additionally, cellular handheld devices typically include Bluetooth, Wi-Fi, and other wireless protocols

capable of joining infrastructure networks or creating dynamic ad hoc networks. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to OHLEG.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of law enforcement officer).
7. Cloning (not as prevalent with later generation cellular technologies).

4.12 Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular devices:

1. Are password protected.
2. Are signed off of OHLEG following each session and before left unattended.
3. Have enabled all existing device security features.

4.13 Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms, whether stored or in transit, is restricted to authorized individuals. Whenever possible, electronic media transported outside of a secured facility

should be encrypted to further protect it from unauthorized access. Physical media shall be protected at the same level as the information would be protected in electronic form.

4.14 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or magnetically erase electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). Agencies shall ensure that the sanitization or destruction is witnessed or carried out by authorized personnel. Destruction should be documented and logged.

4.15 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information being compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure that the disposal or destruction is witnessed or carried out by authorized personnel. Bulk destruction of protection media performed by third party contractors should be documented and logged.

Technical Compliance

5.0 Device and Resource Protection Guidelines

1. Agency management shall ensure that any computer and/or network used to access AGO/BCI/OHLEG information resources does not contain security tools that could be directed to AGO/BCI/OHLEG information resources. Security tools are those used to perform analysis of vulnerabilities in computer systems as well as simulate network or computer attacks that could be detrimental to OHLEG.
2. Agency management shall acknowledge that OHLEG management reserves the right to deny the agency access to AGO/BCI/OHLEG information resources if an event is noted that could potentially put the AGO/BCI/OHLEG information resources or data at risk.

3. Agency shall take reasonable measures to ensure that the agency network and all devices accessing AGO/BCI/OHLEG information resources are secure and free from malicious code.
4. Agency shall have a documented Security Policy that includes but is not limited to the following standards: password controls; user account activation and deactivation process; Incident Process and Procedure; and requirements for end point and perimeter protection, which include but are not limited to the following measures: Antivirus Software, Anti-malware Software, Disk Encryption, Personal Computer Firewalls, Personal Computer Intrusion Detection Software and Intrusion Prevention Software.
5. Agency management shall consent to requests for review of any equipment used to access AGO Information Resources.
6. Agency shall consent to review of security controls or provide adequate documentation upon request.
7. All devices used to access AGO/BCI/OHLEG information resources shall have up-to-date antivirus software running at all times, employ the use of firewalls and have all security related operating system patches applied, and supported internet browser versions installed and updated with all vendor security patches. BCI/OHLEG and/or AGO ITS administration reserves the right to deny access to any device that does not comply.
8. Users shall not download, install, or run security programs or utilities including but not limited to password cracking programs, packet sniffers, or port scanners that attempt to reveal or exploit weaknesses in the security of an AGO/BCI/OHLEG information resource unless approved by AGO ITS Security.
9. Users shall not use shareware or freeware software without the appropriate management approval from their respective agency. Any such software must not permit access to any AGO/BCI/OHLEG data or resources.
10. Users shall not make unauthorized copies of AGO/BCI/OHLEG-owned software, data, or attributes.

11. Users shall not engage in activity that may degrade the performance of AGO/BCI/OHLEG information resources; deprive an OHLEG user access to AGO/BCI/OHLEG information resources; obtain extra resources beyond those allocated; or circumvent AGO/BCI/OHLEG information resources security measures.

5.1 Data Security Threat Incident Response

Agencies shall track and document malicious computer attacks and report such attacks to the BCI/OHLEG Support Center. The OHLEG OAC shall:

1. Be the primary point of contact for interfacing with OHLEG concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Establish procedure for incident reporting in their absence.

Additionally, users shall report any known weaknesses in computer security to the appropriate agency security staff. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.

Appendix A: OHLEG Practice and Test Inquiries

Vehicles:

License Plate #s – TST0001 through TST0069

Ohio BMV Driver's License Records:

SSN – 777-77-7775

OLN – ZZ0000000, ZZ0000015, ZZ0000083

Ohio BMV Image Records:

OLN – ZZ00000007 and ZZ0000520

BCI CCH Test Record:

Name – Public, John Q

Sex – Male

Race – White

DOB – 12/11/1946

BCI# – A123456

Appendix B: Model OHLEG Policy

Agencies are strongly encouraged to develop their own policies to augment the OHLEG security policies. The following are suggested policy statements for an OHLEG Participating Agency's supplemental OHLEG policy. The term CEO refers to an agency's highest ranking administrative official such as a police chief or sheriff. This model policy is available so that each user agency can have an example to reference as it fits these procedures and terminology into the agency's current structure and directives.

The following agency rules apply to the use of OHLEG by any agency member.

The Ohio Attorney General's Office grants agencies and individuals the access to and use of OHLEG exclusively for criminal justice purposes. By virtue of user agreements, the Smallville Police Department and its officers agree to the strict adherence to OHLEG security policies. Individual non-compliance with OHLEG security policies can result in loss of OHLEG access not only for the individual but also potentially for the entire agency. In order to ensure compliance with OHLEG rules and proper usage the Smallville Police Department has created this OHLEG use policy. This OHLEG policy is meant to supplement the existing OHLEG security policies. If there is any question of conflict with the OHLEG rules, the most restrictive interpretation of the OHLEG rules should be applied.

OHLEG use is governed by provisions of the Ohio Revised Code and by the OHLEG security policies (Ohio Rev. Code §§109.57 and 2913.04). Any violations of these rules or misuse or abuse of OHLEG privileges by any member of the Smallville Police Department will be considered a serious violation of agency policy and result in disciplinary action up to and including termination of employment. In addition, violations of the Ohio Revised Code will be referred to the appropriate county prosecutor for criminal prosecution.

In order for any employee at the Smallville Police Department to obtain OHLEG access, the individual must first watch the OHLEG Security Training Video and then submit a request for OHLEG access in writing to his or her supervisor. The supervisor—or an existing OHLEG user—will then fill out an OHLEG application for the individual through the OHLEG Online Account Application process. The applicant will then be required to personally enter his or her name, social security number, and date of birth. The application will then go to the Agency Approver, who will ensure the individual has watched the OHLEG Security Training Video

and signed the OHLEG Agency/User Agreement, select which attributes the individual should have access to, and send the application to the BCI/OHLEG Support Center. Once the individual's application is approved, he or she will be able to access OHLEG.

A copy of the OHLEG security policies will be made available to all approved users of OHLEG. OHLEG users will be held responsible for understanding the contents of the OHLEG security policies, as well as for applying these rules in their use of OHLEG. Agency users will be required to sign a statement indicating they have read and understand the OHLEG security policies before being granted OHLEG access.

OHLEG user authorizations are granted to individual agency members for their exclusive use. All OHLEG transactions are monitored by BCI and subject to audit procedures to verify proper usage and detect violations. Agency members are prohibited from:

- 1) Allowing any unauthorized person to access OHLEG;
- 2) Sharing or giving their sign-on credentials to any other person;
- 3) Leaving their sign-on credentials unprotected in such a way that another person might obtain them; and
- 4) Leaving a computer which has open access to OHLEG unattended and available to unauthorized personnel.

The use of OHLEG is strictly limited to criminal justice purposes. Agency members will be granted access to specific OHLEG attributes based on the particular needs of their job assignment.

Use of OHLEG for anything other than a criminal justice purpose is strictly forbidden. An OHLEG user is not permitted to use an attribute for which he or she has not been given access. Criminal Justice Information (CJI) obtained through OHLEG is also protected and is not to be shared with any unauthorized person.

The agency's OHLEG Agency Coordinator (OAC) is responsible for assisting the CEO with overseeing compliance with OHLEG security policies.

OHLEG access is not permitted outside of normal working hours unless specifically authorized by the OAC.

OHLEG access is not permitted from non-agency computers unless specifically authorized by the OAC.

Anyone becoming aware of an agency member using OHLEG in violation of agency or OHLEG security policies, or in a manner inconsistent with state or federal law, shall report said violation to a superior officer as soon as possible.

If an agency member becomes aware of themselves having committed an OHLEG violation, they are to self-report the violation to their supervisor and the OAC so the violation can be documented. The circumstances that gave rise to the violation can then be examined to determine if there is a need for additional training. Self-reporting a violation does not relieve the user from responsibility for committing the violation.

All OHLEG violations will be reported to the BCI/OHLEG Support Center by either the CEO or OAC.

Any OHLEG violations that rise to the level of a criminal offense will be investigated by the agency, BCI, and/or such outside agencies as deemed appropriate. The results of said investigation will be referred to the county prosecutor for consideration of criminal charges. Violations of the OHLEG restrictions in the Ohio Revised Code are a fifth degree felony.

The OAC shall be responsible for training, applications, policy oversight, and internal audits. Internal audits will be conducted (monthly, quarterly, on an ongoing basis) with a copy of said audit results kept on file in the CEO's office. All violations of this agency policy, OHLEG rules, or Ohio law will be reported to the CEO. The report will include a description of the violation, frequency of occurrence, immediate steps taken to correct the situation, mitigating factors, and an indication of whether additional agency or individual training is needed. The violation and a report on agency action will be forwarded to OHLEG.

Access to OHLEG is a job-specific authorization. Consequently, if an OHLEG user is promoted, transferred, or otherwise experiences a change in duties, they must notify the OAC as soon as possible so the level of their OHLEG authorizations can be evaluated in light of their new assignment. If a member is terminated, their

ability to lawfully access OHLEG is immediately ended, and they are prohibited from accessing OHLEG for any reason. If a member is suspended from duty, they are not permitted to access OHLEG for any reason until such time as they are reinstated to full duty status. If a member is off duty due to sickness, injury, or disability, they are not to access OHLEG for any reason without receiving authorization from the OAC.

Appendix C: Referenced Ohio Revised Code

OHLEG Relevant Sections of Ohio Revised Code

109.57 Duties of superintendent

(C)(1) The superintendent may operate a center for electronic, automated, or other data processing for the storage and retrieval of information, data, and statistics pertaining to criminals and to children under eighteen years of age who are adjudicated delinquent children for committing an act that would be a felony or an offense of violence if committed by an adult, criminal activity, crime prevention, law enforcement, and criminal justice, and may establish and operate a statewide communications network to be known as the Ohio law enforcement gateway to gather and disseminate information, data, and statistics for the use of law enforcement agencies and for other uses specified in this division. The superintendent may gather, store, retrieve, and disseminate information, data, and statistics that pertain to children who are under eighteen years of age and that are gathered pursuant to sections 109.57 to 109.61 of the Revised Code together with information, data, and statistics that pertain to adults and that are gathered pursuant to those sections.

(4) The attorney general may adopt rules under Chapter 119. of the Revised Code establishing guidelines for the operation of and participation in the Ohio law enforcement gateway. The rules may include criteria for granting and restricting access to information gathered and disseminated through the Ohio law enforcement gateway. The attorney general shall permit the state medical board and board of nursing to access and view, but not alter, information gathered and disseminated through the Ohio law enforcement gateway.

The attorney general may appoint a steering committee to advise the attorney general in the operation of the Ohio law enforcement gateway that is comprised of persons who are representatives of the criminal justice agencies in this state that use the Ohio law enforcement gateway and is chaired by the superintendent or the superintendent's designee.

(D)(1) The following are not public records under section 149.43 of the Revised Code: (b) Information, data, and statistics gathered or disseminated through the Ohio law enforcement gateway pursuant to division (C)(1) of this section...

<http://codes.ohio.gov/orc/109.57>

2913.04 Unauthorized use of property - computer, cable, or telecommunication property

(D) No person shall knowingly gain access to, attempt to gain access to, cause access to be granted to, or disseminate information gained from access to the Ohio law enforcement gateway established and operated pursuant to division (C)(1) of section 109.57 of the Revised Code without the consent of, or beyond the scope of the express or implied consent of, the superintendent of the bureau of criminal identification and investigation.

(I) Whoever violates division (D) of this section is guilty of unauthorized use of the Ohio law enforcement gateway, a felony of the fifth degree.

<http://codes.ohio.gov/orc/2913.04>

149.433 Exempting security and infrastructure records.

(A)(3) "Security record" means any of the following: (a) Any record that contains information directly used for protecting or maintaining the security of a public office against attack, interference, or sabotage...

(B) A record kept by a public office that is a security record or an infrastructure record is not a public record under section 149.43 of the Revised Code and is not subject to mandatory release or disclosure under that section.

<http://codes.ohio.gov/orc/149.433>

109.88 Investigation of telecommunications and telemarketing fraud.

(A) If the attorney general has reasonable cause to believe that a person or enterprise has engaged in, is engaging in, or is preparing to engage in a violation of any provision of section 2913.04 or 2913.05 of the Revised Code, the attorney general may investigate the alleged violation.

<http://codes.ohio.gov/orc/109.88>

From: VDowdy@dps.ohio.gov
To: [Stone, Rick](#)
Cc: LEADSSecurity@dps.ohio.gov
Subject: LEADS Access
Date: Friday, February 2, 2024 4:02:17 PM
Attachments: [image001.png](#)
[Cleveland LEADS Access Letter \(003\).pdf](#)

You don't often get email from vdowdy@dps.ohio.gov. [Learn why this is important](#)

Hello,

Please see attached.

Let me know if you have any questions.

Thanks!

Victoria L. Dowdy

Training Program Manager/Acting LEADS Administrator

Ohio State Highway Patrol/LEADS

1970 West Broad Street

Columbus, OH 43223

Phone – 614-752-4381

Cell – 614-420-4737

Fax – 614-995-1230

vdowdy@dps.ohio.gov





Major Matthew Them, Chair, LEADS Steering Committee

LEADS STEERING COMMITTEE

- Sheriff Randy Thorp
 - Judge Beth W. Cappelli
 - Superintendent Joe Morbitzer
 - Chief Vincent Molnar
 - Captain Dennis Swingley
 - Sheriff Matthew Hafey
 - Chief Gary D. Lewis, Jr.
-

February 2, 2024

Cleveland Division of Police
Acting Lieutenant Rick Stone
2001 Payne Avenue
Cleveland, Ohio 44114

Dear Acting Lt. Stone:

LEADS has denied the request to permit civilian public safety employees to review Criminal Justice Information (CJI) since they are not authorized recipients and the purpose does not qualify as the administration of criminal justice.

Per LEADS Administrative Rule 4501:2-10-01 Definitions (A): "Administration of criminal justice" means the detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders.

Per LEADS Administrative Rule 4501:2-10-06 Dissemination and Record Keeping (C): Messages and/or throughput of any kind accessed through LEADS shall be restricted to the use of duly authorized law enforcement and/or criminal justice agencies for the administration of criminal justice.

You can reference the LEADS Administrative Rules and the FBI CJIS Security Policy further at www.leads.ohio.gov.

If you have any further questions, please don't hesitate to contact me at 614-420-4737 or vdowdy@dps.ohio.gov.

Sincerely,

A handwritten signature in cursive script that reads "Victoria Dowdy".

Victoria Dowdy
Acting LEADS Administrator

From: [Griffin, Mark](#)
To: [Racine, Karl](#); [Wilhelm, Abby Jae](#); [Mygatt, Timothy \(CRT\)](#); [Fitzgerald, Patricia M. \(USAOHN\)](#)
Cc: [Thomas, Delante](#); [Johnson, Carlos](#); [Anderson, Leigh](#); [Macias, Hannah](#); [Todd, Dorothy](#); [Drummond, Dornat](#); [Carney, Brian](#)
Subject: [EXTERNAL] Letter from Maj. Matthew Them, LEADS Steering Committee
Date: Friday, March 1, 2024 12:26:48 PM
Attachments: [0460_001.pdf](#)

Attached please find correspondence from Maj. Matthew L. Them, Chair of the LEADS Steering Committee

LEADS



Major Matthew Them, Chair, LEADS Steering Committee

LEADS STEERING COMMITTEE

- Sheriff Randy Thorp
- Judge Beth W. Cappelli
- Chief Vincent Molnar
- Captain Dennis Swingley
- Sheriff Matthew Hafey
- Chief Gary D. Lewis, Jr.
- Director Shane McCracken
- Superintendent Bruce Pijanowski

February 28, 2024

Mark Griffin
Law Director
City of Cleveland
601 Lakeside Ave., Room 106
Cleveland, Ohio 44114-1077

RE: *United States v. City of Cleveland*, 1:15-CV-1046
Monitoring Team and Department of Justice Access to Cleveland Division of Police Records and Systems

Mr. Griffin:

I am in receipt of the letter dated February 23, 2024 from Department of Justice Deputy Chief Timothy Mygatt. LEADS will not issue guidance that conflicts with a court order or agreements reached between the Department of Justice and the Federal Bureau of Investigation's Criminal Justice Information Services Division.

Sincerely,

Major Mathew L. Them
Chair
LEADS Steering Committee